Updated to include
Appendix F: 2023 Digital
Asset Business Risk
Assessment Report

BERMUDA - REPORT ON 2020 MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENTS

GOVERNMENT OF BERMUDA
Ministry of Finance

NATIONAL ANTI-MONEY LAUNDERING COMMITTEE
April 2023

BERMUDA - REPORT ON 2020 MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENTS

GOVERNMENT OF BERMUDA

Ministry of Finance

NATIONAL ANTI-MONEY LAUNDERING COMMITTEE

April 2023

Table of Contents

Disclaimer: This report is produced by the National Anti-Money Laundering Committee. Although the tool used is the World Bank's Model for National Risk Assessments on Money Laundering and Terrorist Financing, the World Bank did not participate in this assessment, nor provide any input into the analysis or conclusions arrived at.

Back to Table of Contents

Foreword

This Report on Bermuda's third cycle of ML and TF national risk assessments from 2020 shows a review that was even more wide-ranging than in previous years, providing analysis of risks to Bermuda that help to further strengthen our already robust AML/ATF framework. Since conducting its first national money laundering (ML) and terrorism financing (TF) risk assessments, in 2013 and 2016 respectively, the Government of Bermuda has reaffirmed this jurisdiction's commitment to compliance with anti-money laundering and anti-terrorism financing international standards. We have also recognised the growing sophistication of criminal activity and cross border threats in this context. Consequently, each review cycle has involved improved data and qualitative inputs, in order to identify, assess and understand ML and TF threats and related risks to Bermuda. Our proactive approach has also extended to identifying evolution in financial sector products and services relevant to our market and regulatory environment. The most recent example would be digital assets. As a result, after being one of the first countries globally to establish a comprehensive licensing regime for the digital asset industry, we have followed up by initiating an ML and TF risk assessment for this aspect of our market. This is taking place in parallel to our ML/TF risk assessment for legal persons, further aligning our 70-year history of robust regulatory oversight in relation to beneficial ownership with enhanced international transparency standards.

We anticipate the results of these two important assessments to be issued by the end of 2023. They represent the priority Bermuda has always placed on balancing a coherent, compliant and effective regulatory approach with appropriate business development strategies, while monitoring and adapting to a continually changing environment. With respect to combating money laundering and terrorism financing, Bermuda continues to recognise the need for all jurisdictions to remain vigilant and support global regulatory developments. This unity of purpose grows ever more important in order to protect national and global economies, as international threats in this context continue to change.

We have proactively reviewed and enhanced our economic, legal and regulatory frameworks, to best understand the risks Bermuda faces. We fully appreciate the need to comprehensively understand ML/TF threat exposures and risks in a constantly changing environment. In fact, Bermuda is to date one of only two jurisdictions to have achieved the Financial Action Task Force's highest rating of "Highly Effective" for our sound and credible understanding of the money laundering and terrorist financing risks we face, and for developing and implementing appropriate risk-focused policies to combat these crimes.

This progressively deeper understanding has enabled us to adapt our frameworks to address those risks with appropriate regulatory policy, market supervision, law enforcement and prosecutorial responses. All these factors contribute to the reputation we have earned as a leading international financial centre. Therefore, our priority

Back to Table of Contents

remains to ensure that Bermuda cannot be used as a base or transit point for illicit proceeds or other related criminality.

I am pleased to note that the analysis in this Report reflects how Bermuda's risk assessments have evolved further in their sophistication, effectiveness and depth of stakeholder cooperation. Once again, all competent authorities with statutory responsibilities for Bermuda's anti-money laundering and anti-terrorist financing regime conducted the extensive analysis involved, led by the National Anti-Money Laundering Committee. This work was also facilitated with the cooperation of the private sector, who were supportive in their responses to comprehensive data requests and provided useful insights as market participants. My Cabinet colleagues and I extend our appreciation to everyone who contributed to this Report. This Report formally documents the analysis that has since been shared with the various financial and non-financial sectors in Bermuda, and has already informed ongoing AML/ATF developments from a public and private sector standpoint. Regulated entities can continue using this as a reference to build further on their own AML/ATF frameworks and systems. And the outcomes from this round of analysis have already been incorporated into the National Strategy and Action Plan for implementation. This Government remains determined to keep protecting Bermuda's economy and borders from illicit financial activity, and to manage related risks appropriately. It remains incumbent on everyone, nationally and internationally, to stay up-to-date on developments in this space as they relate to their particular circumstances and individual entities, and Bermuda will ensure we maintain our hard-earned status as a well-regulated, quality jurisdiction.

The Hon. E. David Burt, JP, MP
Premier of Bermuda and Minister of Finance

Back to Table of Contents

Executive Summary

Publishing this Report has represented a milestone, and anticipated a turning point, in Bermuda's ongoing commitment to combating money laundering and terrorism financing.

For many years Bermuda has played an active role in global anti-money laundering and anti-terrorism financing (AML/ATF) initiatives. Over the past decade in particular, Bermuda has proactively reviewed and enhanced our own robust AML/ATF regulations and operational framework, informed by our first money laundering (ML) risk assessment in 2013. That milestone was followed by an initial analysis of terrorist financing (TF) risk in 2016, and another ML risk assessment in 2017. Since 2017, Bermuda has also undergone a separate, comprehensive assessment of our regime - the 4th Round Mutual Evaluation, conducted by the Caribbean Financial Action Task Force in 2018 and the report published in 2020. The evaluation affirmed the effectiveness of Bermuda's regime, particularly regarding national coordination and policy, domestic cooperation, financial intelligence, transparency of legal persons and arrangements, targeted financial sanctions for TF and the supervision of financial institutions and designated non-financial businesses and professions. Therefore, Bermuda's 2020 national risk assessments, as detailed in this Report, provided another opportunity to update the analysis of our framework and the jurisdiction's risk profile, while supporting continuous improvement.

However, we also continued to recognise the ongoing evolution of financial services, particularly with respect to digital assets, along with FATF developments regarding the transparency of legal persons and beneficial ownership. Bermuda therefore began the process to address both these developments within our AML/ATF framework, by commencing specialized risk assessments for digital asset businesses and legal persons, respectively. The importance of initiating these particular additional risk assessments cannot be overstated. Bermuda can apply its long-standing experience in pragmatic financial regulation to assess, identify and understand ML and TF risks in these areas. For digital assets this builds on our progressive approach, adding to the innovative licensing regime we established for such businesses. For legal persons, Bermuda has always maintained a quality over quantity perspective to the size of our company register and has continually enhanced relevant regulatory requirements. However, updating our understanding of ML/TF risks related to legal persons is seen as another practical opportunity to help enhance the effectiveness of that regime overall. Therefore, these assessments will help to further protect and reinforce the quality of business conducted in the jurisdiction. They will also help Bermuda maintain and demonstrate our active commitment to evolving international standards.

This work is in progress, and generally represents another forward-looking turning point for all jurisdictions to stay abreast of the evolving environment of potential global ML/TF risk. The results of Bermuda's ML/TF risk assessments with respect to digital assets and legal persons will be incorporated as an addendum to this Report later this year.

This Report on the National ML/TF Risk Assessments 2020 (2020 NRAs) focuses on inherent ML risk, includes analysis at national and sectoral levels and, for the first time, comprehensively covers the scale and direction of ML cross-border threats. From the 2020 ML risk assessment, Bermuda's national ML threat rating was raised

Back to Table of Contents

to High from the 2017 rating of Medium-High. This reflected a progressively better understanding of ML threats to Bermuda, and deeper analysis of more comprehensive data and information, rather than any major changes in the threat profile per se. It also reflected the even greater expertise and experience Bermuda has gained for such assessments.

Similar to 2017, crimes perpetrated overseas such as fraud, corruption and bribery, market manipulation/insider trading and international tax crimes were found to present the highest ML threat to Bermuda. Bermuda's financial institutions and the large volume of international services they provide to clients could be impacted by potential money laundering derived from these foreign offences. Domestically, the threat of potential money laundering is still driven by local drug trafficking, and emerging threats from activity such as cyber-based extortion targeting Bermuda residents from overseas were evident. However, the scale of ML threats to Bermuda from foreign predicate offences remains significantly higher.

In the sectoral threats and inherent vulnerabilities assessments, only the Trust sector was rated as High for inherent ML risk, up from Medium-High in 2017. This higher rating reflects deeper analysis showing potential threats and inherent vulnerabilities around misuse of Private Trust Companies for ML purposes. The Deposit-Taking sector (Banks & Credit Union), Corporate Service Providers (CSP), Securities, Long-term (Life) Insurance and Legal sectors were rated as Medium-High. The Real Estate, Betting, Money Service Business and Dealers in Precious Metals and Stones sectors were rated as Medium.

The Lending, General Business/Reinsurance and High Value Goods sectors, along with the Bermuda Stock Exchange, were assessed as Medium-Low risk. The Lending sector was included in the national risk assessment for the first time, as it was brought into scope of the AML/ATF regime in 2018. This sector conducts primarily domestic business, is proportionately small as compared to other financial services sectors and the rating of medium-low risk is consistent with this. The Accounting sector was rated as Low risk. The Casino sector was also rated as Medium-Low risk at this time, reflecting the fact that there are as yet no casino operators in Bermuda; but this preliminary assessment of the sector is beneficial and will inform the supervisory approach once a casino licence is issued.

The nature of the ML threats Bermuda faces is high, particularly given the impact potential money laundering could have on the financial services sector. In common with all financial jurisdictions, Bermuda must be responsive to such threats, but it also understands the current and future benefits of continuing to enhance its already strong AML controls.

Regarding terrorist financing, the TF risk to Bermuda was again assessed to be Low. There was no domestic or foreign-sourced intelligence to suggest that terrorist financing has occurred in Bermuda in any sector. TF threat was also rated as Low across the relevant sectors, other than the banking, MSB and NPO sectors, which were rated Medium-Low. There was no evidence indicating Bermuda has significant inherent threat as a site for domestic or foreign terrorist activity, or is a transit point to move funds from one country to another. Nevertheless, Bermuda's ATF regime remains robust, and the Bermuda authorities are vigilant, recognising that no jurisdiction is completely immune to TF threats and terrorist activities.

Back to Table of Contents

Work to enhance relevant AML/ATF controls across the financial sectors as necessary is ongoing, as part of the national strategy and evolving action plan established formally in 2016 for that purpose. Legislative, institutional and operational changes have already taken place based on previous assessments. The findings from the 2020 NRAs will help inform the next round of updates to the action plan. With Cabinet's approval, all competent authorities responsible for executing the various items incorporated into the action plan are required to align their agency action plans accordingly, and to include them in their accountability reports going forward.

Overall, both government institutions and the private sector can use the results of this risk assessment to ensure they modify their respective risk-based approaches to AML/ATF activities. For intelligence and law enforcement, this means focusing on financial crimes generated via the financial services sector, and for supervisors maintaining their robust monitoring of sectors and entities, particularly those presenting the highest inherent vulnerabilities. For the private sector, the 2020 NRA findings can inform their own ML/TF risk assessments and identify areas for enhanced focus and attention within their institutions. In this way, and with a collective commitment to compliance with international standards, vigilance and continued hard work, Bermuda will stay at the forefront of combating money laundering and terrorist financing.

Back to Table of Contents

Chapter 1: Introduction and Context

Bermuda has used each ML and TF risk assessment conducted since 2013 to deepen its understanding of such risks to the jurisdiction. The Government of Bermuda and relevant supervisory authorities with AML/ATF responsibilities have demonstrated a progressively higher level of understanding and appropriate response to the risks Bermuda faces. Engagement with, and input from, the private sector has also been part of this process, to ensure industry is aware of ML and TF vulnerabilities, can comply with relevant requirements and develop their own risk assessment measures.

As a result of this collective commitment to analyse and combat ML and TF risks, Bermuda's risk-based AML/ATF framework has evolved and continually strengthened. Additional robust policies, strategies and resources have been built up appropriately to combat an equally changing risk landscape. Requirements and guidance from the Financial Action Task Force have been the basis for this evolution, to maintain compliance with international standards. Understanding the context and elements of the jurisdiction's position as an international financial centre, to ensure regime changes are practical as well as effective, has also been essential.

No jurisdiction is totally immune from ML and TF risks, and with this latest National Risk Assessment Bermuda has demonstrated that it remains vigilant. This work has been conducted to ensure Bermuda continues to identify, assess and address ML and TF threats effectively, while reinforcing its position as a leading financial centre.

Relevant FATF requirements

The Financial Action Task Force (FATF) remains the acknowledged international standard setter for AML/ATF matters. The FATF Recommendations and associated Methodology list the requirements for framework and mechanisms that jurisdictions and their relevant public and private sector agencies must have in place to combat money laundering, proliferation and terrorist financing.

FATF Recommendation 1 states, in part:

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a Risk-Based Approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk based measures throughout the FATF Recommendations.

Back to Table of Contents

Technical Compliance Criteria 1.4 of the FATF Methodology requires that "Countries should have mechanisms to provide information on the results of the risk assessment(s) to all relevant competent authorities, self-regulatory bodies (SRBs), financial institutions and DNFBPs."

Presenting the characteristics of an effective system, the FATF's Effectiveness Methodology states that "A country properly identifies, assesses and understands its money laundering and terrorist financing risks, and co-ordinates domestically to put in place actions to mitigate these risks. This includes the involvement of competent authorities and other relevant authorities; using a wide range of reliable information sources."

Bermuda's Geographical Context

Bermuda is located in the North Atlantic Ocean. It is an archipelago of 10 main islands connected by bridges and about 150 additional islets, situated about 570 nautical miles southeast of North Carolina, USA. The archipelago is about 22 miles long with 60 miles of coastline and averages less than 1 mile in width. The capital is the City of Hamilton, with the Town of St. George being the other principal municipality. Bermuda has direct airline service to the UK, Canada and the USA[1]. Flight time to key northeastern US cities is less than two hours. Cruise ships primarily come from the US, with occasional calls coming from the UK and continental Europe.

Bermuda's Political and Judicial Context

Bermuda is a self-governing British Overseas Territory with a parliamentary government. Under its 1968 constitution, the British monarch, represented by the Governor, is the head of state. The Governor is responsible for external affairs, defence, internal security, and the police but acts on the advice of the Cabinet, led by the Premier. The Premier is head of government and of the majority party in the legislature. The legislature is composed of the House of Assembly, with 36 members elected from 36 constituencies to terms of up to five years; and the Senate, with 11 members appointed by the Governor (5 on the advice of the Premier, 3 on the advice of the leader of the opposition, and 3 at the Governor's discretion). While the Senate has the power to defer legislative proposals presented by the House of Assembly for up to one year, it is not empowered to veto or amend any proposed legislation.

[1] Since 2021 an international airline has begun offering seasonal direct flights during the summer between Bermuda and the Azores.

Back to Table of Contents

The Governor formally appoints the Premier, who subsequently nominates Cabinet Ministers and assigns their respective portfolios. The Government currently comprises 11 ministries including the Cabinet Office with responsibility for Government Reform. Cabinet Ministers are each responsible for the operations and strategy of their particular Ministry and are accountable to the Legislature. General elections are held at most every five years, with the most recent being held on October 1st 2020.

Bermuda's legal system is mature and transparent, with an extensive, well-qualified network of legal professionals. The legal system reflects the UK model, comprising codified legislation and English common law. The court system is composed of Magistrate Courts, the Supreme Court, a local Court of Appeal, and final appeal to the Privy Council in the UK.

Bermuda's Economic and Social Context

Bermuda's economy is predominantly based on tourism and international financial services, which represented 5.1% and 25.2% of GDP, respectively, in 2019. Tourism and international financial services employ the majority of the workforce directly or indirectly.

As at the time of this assessment Bermuda had four licensed banks, all serving domestic and international clients. Bermuda's corporate registry has approximately 16,000 registered legal entities, and approximately 1,300 of these are AML/ATF regulated FIs. The Bermuda dollar is pegged to the US dollar at a fixed exchange rate of US$1.00=BD$1.00 (par). Principal trading partners include the US (which predominatesin the volume and value of trade), UK, European Union and Canada.

According to the 2016 Population and Housing Census Report. Bermuda had a population of 63,779, of which 19,332 residents were foreign-born and 9,506 were guest workers from overseas. Guest workers primarily come from the UK, Canada, USA, Azores/Portugal, the Caribbean and Asia.

English is the official language. Education is free and compulsory for students aged 5 - 16. Literacy rates are high, and approximately 87% of the adult population are high school graduates, a large proportion of whom go on to higher education, either in Bermuda or abroad.

Back to Table of Contents

Chapter 2: Bermuda's AML/ATF Legislative Framework and Key Agencies

Legislative Framework

Bermuda has a comprehensive suite of legislation to combat money laundering and the financing of terrorism.

Core Legislation

Key laws in relation to AML/ATF include:

i. **Proceeds of Crime Act 1997 (POCA)** – *This Act establishes the criminal offences that constitute money laundering, sets the legal framework for confiscating proceeds of crime and confers investigative power on the police. The Act also confers expansive information-gathering powers to the police relating to investigations and contains provisions empowering the courts to make confiscation orders, forfeiture orders and freezing orders and to impose other penalties. It contains the provisions relating to filing of Suspicious Activity Reports (SARs) and provides the legislative basis for regulations to impose requirements on specified Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) for preventive measures in relation to AML/ATF matters. It also contains the legislative basis for the Minister responsible for Justice to give directions in relation to matters that have significant ML/TF risk. It establishes the National Anti-Money Laundering Committee (NAMLC) and establishes the civil recovery regime which provides for the Enforcement Authority to recover funds that are the proceeds of criminal conduct.*

ii. **Anti-Terrorism (Financial and other Measures) Act 2004 (ATFA)** – *This Act criminalises the financing of terrorism and establishes a series of offences relating to involvement in arrangements for facilitating, raising or using funds for terrorism purposes. The Act also confers information gathering powers on the police and empowers the courts to make orders and impose penalties in relation to investigations relating to terrorism offences. It also contains relevant provisions in relation to TF and Proliferation Financing (PF) matters that appropriately mirror those relating to ML that are contained in POCA.*

iii. **Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (Regulations)** – *This legislation was established in accordance with POCA and ATFA. The regulations prescribe the preventive measures to be taken by AML/ATF regulated FIs and regulated Non-Financial Businesses and Professions (DNFBPs).*

Back to Table of Contents

iv. **Proceeds of Crime (Anti-Money Laundering and Anti- Terrorist Financing Supervision and Enforcement) Act 2008 (SEA)** – *This Act establishes the supervisory framework whereby supervisory authorities are required to monitor certain persons and take measures to secure compliance by such persons with the regulations made under the Proceeds of Crime Act 1997 and the Anti-Terrorism (Financial and Other Measures) Act 2004. The responsibilities and powers of supervisory authorities are prescribed, as well as the civil penalties for breach of the Regulations.*

v. **Financial Intelligence Agency Act 2007** – *This Act established the FIA as the national Financial Intelligence Unit (FIU) as an independent, autonomous agency to receive reports of suspicious transactions from regulated financial institutions and other persons and to collate, analyse and, as appropriate, disseminate information to law enforcement and other competent authorities for investigation or other action.*

vi. **Criminal Code Act 1904** – *This Act criminalises a wide range of offences, which comprise the majority of the predicate offences for money laundering; and establishes the framework for charge, prosecution and sentencing of all offenders.*

vii. **Misuse of Drugs Act 1972** – *This Act criminalizes a wide range of drug trafficking offences and provides additional police powers for investigating such offences including forfeiture orders.*

viii. **Bribery Act 2016** – *The Bribery Act amalgamates all bribery offences, including bribery of a foreign public official. The Act also prescribes the procedure for reporting, prosecution and penalties.*

ix. **Revenue Act 1898** – *This Act provides the regulatory regime for Customs and confers appropriate powers on the Collector of Customs.*

x. **Companies Act 1981** – *This Act provides the framework for the incorporation, registration, and winding-up of companies. Other legislation which relate to the establishment and operation of other types of legal entities in Bermuda include the Partnership Act 1902; the Limited Partnership Act 1883; the Exempted Partnerships Act 1992; the Overseas Partnerships Act 1995; the Limited Liability Company Act 2016; and the Segregated Accounts Companies Act 2000.*

Back to Table of Contents

These Acts are reinforced and supported by the Registrar of Companies (Compliance Measures) Act 2017, which confers powers on the Registrar of Companies to better provide for inspection of, and compliance by, certain entities that are registered in Bermuda.

xi. **Exchange Control Act 1972** – *This Act provides the regulatory framework for exchange controls and includes provisions that allow for the vetting of beneficial owners. This Act and the Exchange Control Regulations 1973 are important components of Bermuda's long-standing history of knowing and vetting the key players behind companies registered in Bermuda.*

xii. **Charities Act 2014** – *The Charities Act imposes a registration framework for charities and establishes a risk-based supervisory framework for registered charities, to ensure compliance with regulations that prescribe the AML/ATF obligations on charities: namely, the Charities (Anti-Money Laundering, Anti-Terrorist Financing and Reporting) Regulations 2014.*

xiii. **Criminal Justice (International Cooperation) (Bermuda) Act 1994** – *This legislation establishes the framework to enable Bermuda to provide legal assistance, evidence and other material support, to cooperate with other countries in the investigation and prosecution of criminal offences and the detention and recovery of criminal proceeds.*

xiv. **International Cooperation (Tax Information Exchange Agreements) Act 2005** – *This Act makes general provision for the implementation of tax information exchange agreements entered into by the Government of Bermuda, as authorised by the Government of the United Kingdom, with other jurisdictions and to enable the Minister of Finance to provide assistance to the competent authorities of such jurisdictions under such agreements.*

xv. **International Sanctions Act 2003** – *The Sanctions Act allows the Minister responsible for legislative affairs to make the necessary regulations for the international sanctions regime. Other relevant Sanctions related legislation include:*

- **International Sanctions Regulations 2013** – *These Regulations, whose legislative basis is derived from the International Sanctions Act, provide the mechanism for Overseas Territories Orders for international sanctions measures (United Nations and others) to be brought into force in Bermuda.*

Back to Table of Contents

- **International Sanctions Notice 2017** – *This Notice confers powers by any provision to any of the Orders listed in Schedule 1 to the International Sanctions Regulations 2013 to maintain and publish a list of designated or listed persons constituting the target of financial sanctions and a list of restricted goods.*

Additional Legislation

In addition to the above core legislation, the framework for monitoring and enforcing compliance is strengthened by measures contained in the primary Acts establishing the supervisory authorities which include the:

i. **Bermuda Monetary Authority Act 1969** – *This Act established the Bermuda Monetary Authority and provides its powers for, among other things, the regulation and supervision of financial institutions and the prevention of financial crime.*

ii. **Gaming Act 2014** – *This legislation provides for integrated resorts, to allow casino gaming, to establish the Bermuda Gaming Commission and to establish a Problem Gaming Council to address problem gambling.*

iii. **Real Estate Brokers' Licensing Act 2017** – *This Act provides for the operation of a licensing regime for the Real Estate sector and establishes the supervisory framework.*

iv. **Registrar of Companies (Supervision and Regulation) Act 2020 and Registrar of Companies (Compliance Measures) Act 2017** – *These Acts empower the Registrar of Companies with supervisory and regulatory authority and powers in relation to a wide range of compliance requirements, with respect to registered persons and entities, as well as in respect of the AML/ATF oversight of dealers in high value goods.*

v. **Bermuda Bar Act 1974 and Chartered Professional Accountants of Bermuda Act 1973** – *These Acts contain provisions relevant to the establishment and operation of the Barristers and Accountants AML/ATF Board and the oversight of persons in the legal and accounting sectors.*

Back to Table of Contents

In addition, the suite of regulatory legislation can also be used as part of the AML/ATF framework and includes the following pieces of legislation:

- *Banks and Deposit Companies Act 1999*
- *Corporate Service Provider Business Act 2012*
- *Insurance Act 1978*
- *Investment Business Act 2003*
- *Investment Funds Act 2006*
- *Money Services Business Act 2016*
- *Trusts (Regulation of Trust Business) Act 2001*
- *Digital Asset Business Act 2018*
- *Digital Asset Issuance Act 2020*

Key AML/ATF Agencies

The Government of Bermuda has, by statute or delegation, designated the following agencies to play a leading role to address AML/ATF matters:

Table 1: Key AML/ATF Agencies (Competent Authorities)

AGENCY	PRIMARY ROLE WITHIN THE AML/ATF REGIME
National Anti- Money Laundering Committee (NAMLC)	• AML/ATF advisory and coordinating body • The Office of NAMLC acts as secretariat for NAMLC and plays a key role in relation to coordination and development of the national policies, framework and programme.
Attorney-General's Chambers (AGC)	• Central authority – Mutual Legal Assistance • Civil asset recovery and civil forfeitures under the POCA
Bermuda Gaming Commission (BGC)	• Supervisory authority for casino gaming, betting and other gaming related activities.
Bermuda Monetary Authority (BMA)	• Supervisory authority for financial sector • Responsibilities in relation to vetting and retaining information on beneficial ownership of legal persons
Bermuda Police Service (BPS)	• Criminal investigations
The Customs Department (Customs)	• Immigration and customs control at all ports of entry
The Department of Public Prosecutions (DPP)	• Criminal prosecutions • Confiscation/forfeiture (conviction based)
Financial Intelligence Agency (FIA)	• Receipt of Suspicious Activity Reports (SAR) and analysis and dissemination of SARs and other financial intelligence
The Ministry of Finance (MoF)	• Authority for exchange of tax information • Domestic tax authority • Minister appoints NAMLC Chair

Back to Table of Contents

AGENCY	PRIMARY ROLE WITHIN THE AML/ATF REGIME
The Ministry of Legal Affairs and Constitutional Reform (MoLACR)	• Minister with key responsibilities under POCA, SEA and ATFA • Minister is the delegated authority for targeted financial sanctions and the Ministry houses a dedicated unit for this purpose – the Financial Sanctions Implementation Unit (FSIU)
The Registry General (RG)	• Supervisory Authority for Charities • Registrar of births, deaths and marriages
The Registrar of Companies (RoC)	• Registration and regulation of legal persons (company registry) • Supervisory Authority for Dealers in High Value Goods, which includes dealers in precious metals and stones
The Superintendent of Real Estate (SoRE)	• Supervisory Authority for real estate brokers and agents
The Barristers and Accountants AML/ATF Board[2] (Board)	• Supervisory Authority for independent professionals – lawyers and accountants

The National Anti-Money Laundering Committee and the Office of NAMLC

NAMLC was established by Section 49 of POCA 1997 and advises Government Ministers on AML/ATF matters. Its role is defined as follows:

- Advising Government Ministers in relation to:
  - the detection and prevention of ML/TF and the financing of proliferation;
  - the development of a national plan of action to include recommendations on effective mechanisms to enable competent authorities in Bermuda to collaborate with each other concerning the development and implementation of policies and activities to combat ML/TF and the financing of proliferation.
- Advising the Government Ministers about Bermuda's participation in the international effort against ML/TF and the financing of proliferation, including the development of policies.

NAMLC consists of a Chair, appointed by the Minister of Finance, and the heads of all of the competent authorities that are primarily involved in AML/ATF matters. Through regular meetings of the committee and its working groups, NAMLC works to ensure that AML/ATF matters are appropriately addressed and facilitates coordination, collaboration and cooperation. There are four permanent working groups established: the Legislative and Policy Working Group, the Supervisory Forum, the Operational Working Group and the Sanctions Working Group.

[2] The Board is a self-regulating organization, so by FATF definition, is not a "competent authority".

Back to Table of Contents

The Office of the NAMLC is the Secretariat for NAMLC and works with NAMLC agencies and other entities to ensure that the mandate of NAMLC is effectively carried out. It plays a key role, on behalf of NAMLC, in coordinating Bermuda's AML/ATF national and multi-agency activities, including national risk assessments and development of national policies.

The Attorney-General's Chambers (AGC)

The AGC, on behalf of the Attorney-General, acts as the legal advisor to the Government and is responsible for mutual legal assistance in responding to foreign requests for formal assistance in criminal matters. The AGC also deals with requests (on behalf of the DPP) to other countries, to assist Bermuda in ML/TF criminal matters.

Acting on behalf of the Mi.nister of Legal Affairs and Constitutional Reform, who is the designated Enforcement Authority, the AGC also plays a key role in relation to civil recovery of assets deemed to be the proceeds of criminal conduct. The AGC also has responsibility for the legal processes involved in other civil forfeitures under POCA.

Bermuda Gaming Commission

The Bermuda Gaming Commission[3] was established in 2015, by the Casino Gaming Act 2014[4] (as it was then named), to regulate casinos in Bermuda. As noted on its website, the Commission has developed five key principles which outline the requirements for a casino to be established in Bermuda. These are: suitability; accountability; integrity; collectability of payments and protection of the vulnerable.

Although no casinos are currently in operation in Bermuda, two entities have been granted provisional licences. However, entities holding such provisional licences are not able to offer gaming services to the public until a comprehensive assessment of the suitability of relevant persons and entities is undertaken and an operating licence has been issued. The Commission has done considerable work in relation to the development of its AML/ATF framework. Regulations to the *Gaming Act 2014* have been enacted to provide direction to casinos and their operators on internal control requirements, policies and procedures necessary to manage ML/TF risks.

Bermuda Monetary Authority (BMA)

The BMA was established by the Bermuda Monetary Authority Act 1969 as the sole financial services regulatory body in Bermuda. In addition to the core financial sectors of banking, insurance and investments, the BMA also supervises persons licensed to conduct trust business, such as Trust Service Providers (TSP) and entities licensed to conduct Corporate Service Provider (CSP) business in Bermuda. The BMA is also responsible for supervising financial institutions in order to combat ML and to enforce ATF measures in Bermuda.

[3] By statutory amendment in 2021, the Bermuda Casino Gaming Commission was renamed as "Bermuda Gaming Commission".

[4] This Act was renamed by amendment in 2021, to "The Gaming Act 2014"

Back to Table of Contents

Through its role as a member of NAMLC, the BMA advises the Government on supervisory and regulatory matters relating to financial institutions in order to ensure that robust AML/ATF legislation is in force to effectively carry out its statutory mandate and to meet domestic and international standards and best practices. Further, the BMA develops and issues AML/ATF Guidance Notes to the sectors that it regulates.

The BMA —an independent authority—regulates the following entities in accordance with its powers under the Regulatory Acts and Bermuda's AMF/ATF framework:

- Banks
- Credit Union
- Securities Companies (investment businesses, investment funds and fund administrators)
- Insurance: long-term business insurers (i.e., life and non-life insurers), insurance managers and insurance intermediaries (brokers, salesmen and agents)
- Money Service Businesses
- Trust Service Providers
- Corporate Service Providers
- Digital Asset Businesses

The BMA also has a statutory role in the company incorporation process in Bermuda, including, as appropriate, vetting the applications and keeping the registry of beneficial owners of legal entities on behalf of the Minister of Finance.

Bermuda Police Service (BPS)

The BPS is responsible for investigating crimes. The Organised and Economic Crime team deals with offences of ML/TF and with associated predicate offences. The POCA places responsibilities on the BPS to investigate, trace and confiscate the proceeds of criminal conduct.

The BPS's AML/ATF policy objectives are to:

- ensure that financial investigations become the cornerstone of all major proceeds-generating cases and TF cases
- identify proceeds of crime, trace assets, and initiate asset confiscation measures, and use temporary measures such as freezing/seizing, and restraint powers when appropriate
- initiate ML investigations when appropriate
- uncover financial and economic structures, disrupt transnational networks, and gather knowledge on crime patterns

Back to Table of Contents

The Customs Department (Customs)

The Customs Department is under the control of the Minister of Finance but is subject to the directions and instructions of the Minister of National Security in relation to import and export prohibitions.

Customs was established under the *Customs Department Act 1952*. Customs has border control and protection responsibilities, the key powers of which are contained in the *Revenue Act 1898* In relation to the processing of incoming passengers, customs officers carry out the primary traveler screening process for the Department of Immigration.

The Department's main responsibilities are:

- facilitation of legitimate trade
- assessment and collection of duty revenue
- interdiction of drugs and other contraband and the proceeds of crime at our borders

The Department of Public Prosecutions (DPP)

The Department of Public Prosecutions is responsible for public prosecutions, confiscation and conviction-based forfeiture of assets. DPP prosecutes criminal offences, including in relation to ML and TF, and advises the BPS, Government departments and the Criminal Injuries Compensation Board.

Financial Intelligence Agency (FIA)

The FIA was established by the *Financial Intelligence Agency Act 2007* to act as an independent agency authorised to receive, gather, store, analyse and disseminate information relating to ML, suspected proceeds of crime and potential financing of terrorism received in the form of Suspicious Activity Reports (SARs). The reporting of suspicious transactions requirements (Section 46 of the *Proceeds of Crime Act 1997* (POCA)) and tipping off provisions (Section 47 of POCA) apply equally to all persons during the course of their business, trade or profession. The FIA has the authority to share relevant information with the BPS, other domestic competent and supervisory authorities and foreign financial intelligence units.

The Ministry of Finance (MoF)

The MoF oversees the economy of Bermuda and has overall responsibility for providing a framework for the financial management and control of Government activities and finances. The Treaty Management and Administration Unit within the MoF acts as the authority for the exchange of tax information and the Office of the Tax Commissioner, which has responsibility for domestic tax matters, is also a department within this Ministry.

Back to Table of Contents

The Ministry of Legal Affairs and Constitutional Reform (MoLACR)

The MoLACR has administrative responsibility for the Attorney-General's Chambers, the Judiciary, Department of Court Services, DPP and Legal Aid Office. The Ministry has overall responsibility for upholding the constitution and legal system of Bermuda, providing legal services together with the efficient delivery and accessibility of justice. MoLACR works closely with the Governor and Government House in relation to international sanctions and PF matters. The Minister has key responsibilities and powers in relation to AML/ATF matters under POCA, ATFA and SEA. All Guidance Notes issued by supervisory bodies are subject to approval by the Minister. In addition, the Minister can issue directions to regulated financial institutions in relation to specified matters involving high ML, TF or PF risk. Matters related to the issuing of regulations prescribing preventive measures for the prevention and detection of ML and TF, also fall within the purview of the Minister.

The Registry General (RG)

The RG became the supervisory authority for charities under the *Charities Act 2014*. The applicable AML/ATF requirements are detailed under the Charities AML/ATF Regulations 2014 and as required by the FATF, allows for a TF focused, risk-based approach, both in relation to the requirements imposed and to the monitoring and enforcement of compliance. This agency is part of the Ministry of Home Affairs, which has oversight of the operation and management of the RG, but in relation to legislative and policy matters these functions come under the remit of the Ministry of Social Development and Seniors.

Registrar of Companies (RoC)

The RoC was established in 1970 and supervises all registered entities (i.e. companies, partnerships, and Limited Liability Companies (LLCs)) formed under the following operative Acts:

- *Companies Act 1981*
- *Partnership Act 1902*
- *Limited Partnership Act 1883*
- *Exempted Partnerships Act 1992*
- *Overseas Partnerships Act 1995*
- *Limited Liability Company Act 2016*
- *Segregated Accounts Companies Act 2000*

The Registrar of Companies *(Compliance Measures) Act 2017* grants the RoC additional power and responsibilities in relation to monitoring and enforcing compliance with legislation that applies to establishing and operating legal entities registered and/or operating in or from Bermuda.

Additionally, the Registrar of Companies (Supervision and Regulation) Act 2020 empowers the Registrar with supervisory authority and powers in relation to dealers in high value goods, taking over from the Financial Intelligence Agency, which previous held and exercised those responsibilities.

Back to Table of Contents

The RoC is also responsible for:

- revenue collection
- providing publicly searchable records of registered entities
- company investigations and complaint resolution
- company winding-ups/strike offs
- handling certain bankruptcies and liquidations

The Superintendent of Real Estate (SoRE)

The SoRE, who is also the Registrar of Companies, was designated under SEA as the supervisory authority for the Real Estate sector in Bermuda in September 2016. At the same time, the sector was brought into scope under the AML/ATF framework. Additional powers and responsibilities in relation to AML/ATF supervision of the sector are contained in the *Real Estate Brokers' Licensing Act 2017*. This Act contains the applicable licensing requirements, including those in relation to "fit and proper" criteria to which the sector is subject, as well as a range of enforcement measures for non-compliance with relevant legislation.

The Barristers and Accountants AML/ATF Board (Board)

The Barristers and Accountants AML/ATF Board (the Board) is a self-regulatory body, established jointly by the professional bodies for the legal and accounting sectors on the basis of their having similar professional codes, client bases and work products. The Board was then established in law under Section 25A of the *Bermuda Bar Act 1974* and Section 8A of the *Chartered Professional Accountants of Bermuda (CPA) Act 1973*. Effective August 10, 2012, the Board was designated as a supervisory authority by order of the responsible Minister, issued under Section 4 of the *Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (SEA)*.

The Board is responsible for supervising Regulated Professional Firms (RPFs) for compliance with the obligations under the AML/ATF Regulations. RPFs is defined to bring into scope independent professionals, namely, accounting firms who are members of CPA Bermuda, and legal firms which advise clients in connection with specified activities.

As the Board is not a government agency nor a public authority, it is not a statutory member of NAMLC. It does, however, work closely with the NAMLC, in addressing matters relevant to the effective development and implementation of the AML/ATF regime. It is a member of NAMLC's Supervisory Forum, attends NAMLC meetings and actively participates in national AML/ATF initiatives.

Back to Table of Contents

Chapter 3: Bermuda's AML/ATF Operational Framework

A. Regulation and Supervision

As highlighted previously, the *Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008* (SEA) provides the legislative underpinning for the AML/ATF supervisory framework for regulated financial institutions and non-financial businesses and professions, as defined in the Regulations. The supervisory bodies that derive their authority from the provisions detailed in SEA are the BMA, BGC, ROC, SoRE and the Board. This chapter provides information on the approach that these supervisors take for monitoring and enforcement of compliance with the relevant AML/ATF requirements. The table below provides information on the nature and size of the AML/ATF regulated sectors.

Table 2: The AML/ATF Regulated Sectors

Sector	**Number of Regulated Entities in Sector** *(as at Dec. 31, 2019)*
Deposit Taking	5
Securities	788
Insurance	1431
Money Service Businesses	3
Gaming	0
Betting	3
Real Estate	51
Dealers in precious metals and stones	0
Accountants	8
Lawyers	30
High-value dealers (Car, boat, motorcycle and antique dealers; and auctioneers)	0
Trust Service Providers	28
Corporate Service Providers	95
Other financials (Bermuda Stock Exchange)	1
Lending	0

Back to Table of Contents

The Bermuda Monetary Authority's Supervisory Framework

The BMA is responsible for licensing and supervising with regard to both financial stability (i.e. prudential matters) and for AML/ATF purposes, and setting out the AML/ATF control obligations for the sectors it supervises.

Its supervisory framework provides a comprehensive risk-based approach to AML/ATF supervision across those sectors and entities it regulates. The BMA used the FATF Recommendations and guidance[5] as the basis for developing this risk-based supervisory framework and is committed to continuous engagement with FATF direction, in order to maintain a credible deterrent to ML/TF within its scope of responsibilities.

The BMA's AML/ATF supervisory framework comprises the following components:

1. Assessment of ML/TF risks and controls – to inform planning
2. Licensing and authorisations – to effect market entry controls
3. Regulation and information – to guide and inform regulation and regulated FIs
4. Offsite and onsite supervision – to assess the quality of controls for regulated FIs
5. Enforcement – to proportionately address breaches of requirements
6. Monitoring and reporting – to ensure ongoing effectiveness of supervisory actions on compliance

Assessment of ML/TF risks and controls

The BMA conducts, or provides input to, ML/TF risk and control assessments at the national, sectoral and entity level. Each of these risk assessments is used to inform and cross-calibrate the overall results. This ensures that the BMA, and other relevant competent authorities in Bermuda, have a consistent, current and holistic view of ML/TF risks.

The BMA develops its understanding of the ML/TF risks facing sectors under its supervision, by conducting an annual risk assessment at both sector and entity levels, using data calls and questionnaires. The risk assessments are structured as follows: understanding the inherent risk within each regulated entity in a sector; assessing the effectiveness of the ML/TF controls in place; estimating the level of residual risk in that entity and aggregating entity results to reflect the sectoral risk profile. This risk assessment is used to inform the Risk-Based Approach (RBA) to AML/ATF supervision across all stages of the AML/ATF supervisory lifecycle. As the process is repeated in an iterative cycle of risk assessment and supervisory activities, the BMA's understanding of residual risk is continually deepened and refined. The results of these risk assessments inform the annual calendar of supervisory activities and requirements, including the development of the BMA's supervision strategies, priorities and resourcing.

[5] 2012 Revised FATF Recommendations and FATF Guidance for a Risk-based Approach "Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement", October 2015. Updated RBA guidance for supervisors from FATF is now also available from the FATF, and is entitled - "Risk-Based Supervision", March 2021.

Back to Table of Contents

Licensing and Authorisations

A key component of the BMA's RBA to supervision relies on robust market entry controls. This is achieved through the BMA's licensing process. The BMA first plays a key "gatekeeper" role in vetting beneficial owners for all companies operating in Bermuda, to address the risk of criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or performing a management function, in any company. The second key role played by the BMA is the licensing process for financial institutions. The market entry controls for financial institutions are based around the determination of beneficial ownership, assessment of fit and proper shareholder controllers, and granting of licensing or registration. The BMA places emphasis—through its licence and registration application process—on ensuring that Bermuda maintains quality-over-quantity of approved financial institutions.

Each of the various regulatory Acts administered by the BMA describes the legislative requirements for the licensing or registration of the respective FIs. All local or overseas FIs (including non-resident insurance companies) are subject to these Acts and are required to apply for and receive a licence, registration or exemption, or where applicable, register an exemption with the BMA before they are able to conduct business in Bermuda.

The licensing process in Bermuda for FIs consists of three stages:

1. **Incorporation**: the BMA conducts vetting as part of the incorporation process, which includes a review of the shareholding and beneficial ownership of the proposed company as well as their suitability, considering any risks to the Bermuda economy.
2. **Licence:** this includes an assessment of controllers—in relation to "fit and proper" criteria, the business plan and governance arrangements, which would include proposed AML/ATF policies and procedures as well as the source of funds.
3. **Ongoing Monitoring**: the BMA conducts ongoing monitoring of minimum licence criteria, including changes in beneficial ownership and controller information and terms of the licence.

Back to Table of Contents

Regulation and Information

The BMA provides relevant input to NAMLC and, as appropriate, to Cabinet on AML/ATF-related legislative and regulatory items. The BMA is also responsible for providing comprehensive guidance to industry on (i) how the AML/ATF regulations will be applied; (ii) the expectations of the BMA for individual sector compliance with the regulations and processes, and (iii) enhancing overall understanding of AML/ATF matters, including AML/TF risks. The BMA has implemented a programme of industry outreach and communications that ensures regular updates on these topics and promotes a collaborative dialogue with industry.

Off-site and On-site Supervision

The BMA employs a risk-based approach to on-site and off-site supervision activities appropriate to the level of ML/TF risk of each supervised sector and their component FIs. The BMA's risk-based framework for AML/ATF supervision is underpinned by the risk profiles of each sector and of their component institutions, as described above. The BMA creates and implements the supervisory plan on an annual basis.

The results of the NRA and the BMA's annual sectoral risk assessments provide the main input for sectoral risk profiling and supervision planning. This enables the BMA to conduct macro sectoral analysis of risk that can be used to prioritise higher-risk sectors for enhanced supervision. Within each sector, the results of the BMA's entity-level risk assessment is used to identify entities with higher-risk profiles for enhanced supervision, taking into account the risk profile of the sectors to which they belong.

The reports arising from supervisory reviews are communicated to the FI concerned, and a formal programme of follow-up is implemented to ensure that matters are addressed in an appropriate and timely manner. If serious deficiencies in an FI's AML/ATF regime are uncovered or remediation deadlines are missed, the RFI may be subject to enforcement action.

Enforcement

The BMA exercises its powers of enforcement to fulfill its function as a supervisor and regulator of financial institutions in Bermuda, to demonstrate its commitment to adhering to international standards and to foster a fair commercial environment in Bermuda. The BMA will take action in accordance with the principles set out in its Enforcement Guide, which include exercising powers in a fair, consistent and proportionate manner. A key guiding principle is that the Authority will apply enforcement sanctions that are dissuasive and proportionate to all of the surrounding circumstances, including risk.

Enforcement actions are specifically intended to address and alleviate failures of compliance or breaches of regulations, and to the BMA's powers to impose dissuasive outcomes. Where the nature

Back to Table of Contents

of the breach is of sufficient seriousness, enforcement measures or as is more typically the case a combination of remediation and enforcement measures may be required. During the period covered by the risk assessment, the BMA used its powers to levy civil fines, issue public and private sanctions and take other regulatory enforcement actions as indicated by specific cases.

Monitoring and Reporting

The BMA carries out ongoing monitoring of the effects of the supervisory process, as it is important to ensure that BMA's supervision is achieving its fundamental objective of improving the AML/ATF compliance of the FIs. The steadily increasing numbers of SARs is one indicator of enhanced compliance in the private sector.

The Registrar of Companies' Supervisory Approach

Amendments made to the SEA, which came into effect on December 1, 2016, initially designated the Financial Intelligence Agency as the supervisory authority for dealers in high-value goods (DiHVG, which include jewelry dealers; car, boat and motorcycle dealers; precious metal and stone dealers; antique dealers and auctioneers). DiHVG were brought into scope of the *Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008* (Regulations), subject to the requirement that they be registered with the FIA if they intend to carry out cash transactions equal to or above BD $7,500, or the equivalent in any other currency. However, subsequent amendments to SEA in 2020, in tandem with the Registrar of Companies ((Supervision and Regulation) Act 2020, transferred responsibilities for the supervision of DiHVGs from the FIA to the ROC. These changes came into effect on 1st November 2020.

Registered DiHVG must also file Cash Transaction Reports (CTRs) with the FIA whenever they carry cash transactions equal to or above BD $7,500. Entities that fall within the definition of DiHVG that are not registered are not authorised to accept cash above this threshold.

Outreach and Training

The ROC has established a reporting entity function which ensures resources are dedicated to awareness raising activities that are targeted and strategic to the DiHVGs sector. Entities within the sector have received this training positively. This outreach and training programme remains an important component of the supervisory approach for this sector.

Back to Table of Contents

Guidance and Communication

There is ongoing communication with the entities in the sector on matters that are relevant to their AML/ATF compliance. Industry representatives were involved in the 2020 ML risk assessment, on which the FIA and ROC collaborated, and communication of the results of the NRA are part of the ROC's continual awareness strategy. At the time of this report, the ROC was preparing to issue its Guidance Notes to the DiHVGs sector.

Supervision and Oversight

At the end of 2019 there were no businesses registered with the FIA as dealers in high value goods. Transfer of responsibilities to the ROC, for supervision of this sectoral group occurred as of 1st November 2020, at which time there were still no registrants, based on the fact that the sector adopted the policy of not accepting cash payments at or above the statutory threshold of $7,500. Therefore, there was no need for businesses in the sector to be registered with the ROC.

The ROC continues to monitor the sector to ensure entities maintain adherence to this cash policy.

As part of the implementation of its new regime, the ROC conducts outreach to the DiHVGs sector to maximise understanding about its AML/ATF obligations. The ROC expects to conduct the first round of policing the perimeter inquiries to unregistered businesses by 31st December 2022.

Risk Assessment

The ROC recognises the importance of ensuring there is a good understanding of the risks in the sector and that this information is kept up to date. In the context of the 2020 national risk assessment process, the ROC consulted with the sector to better understand its ML/TF risks. The ROC has also been conducting research using mass and social media sources, as well as other publicly available information, to identify all entities in the DiHVGs sector. In addition, the ROC plans to conduct a quantitative survey to gather important compliance information to extend its understanding of ML/TF risks within the sector.

Back to Table of Contents

The Superintendent of Real Estate's Supervisory Approach

The Superintendent of Real Estate has adopted a comprehensive approach to real estate sector supervision with activities ranging from education to inspection and corrective action. The supervisory framework includes all tools and functions that will help achieve the highest level of compliance within the sector.

The Superintendent of Real Estate has implemented a risk-based approach to supervision that allows for the appropriate focus of resources on high-risk entities. The six key functions that form the basis of the Superintendent's risk-based supervisory framework are:

- licensing
- risk assessment
- legislative and policy interpretation
- reporting entity assistance
- monitoring and inspections
- corrective actions/enforcement

The goal is to achieve high levels of cooperation and compliance, to contribute to an effective system that will minimise the potential for abuse by those involved in ML/TF activities and also to reduce the need for enforcement actions.

Licensing Framework

The Real Estate Brokers' Licensing Act 2017 establishes a robust licensing regime, which includes fit and proper and other due diligence requirements. Since December 2017, the Superintendent has operated annual licensing for the sector in accordance with these requirements.

Risk Assessment

SoRE conducts annual risk assessment of the sector, both within the national risk assessment processes (2017 and 2020) and as discrete sectoral assessments in intervening years. SORE has worked consistently since 2017, to strengthen the quality of data accessed from licensees in data call and onsite inspection processes to support more robust sectoral and institutional risk profiling. In this regard, the SORE utilises a risk assessment matrix to update the required statistical return. This return is completed and submitted annually by all brokers.

Legislative and Policy Interpretation

The SoRE has issued Guidance Notes to provide further clarification on the requirements in the relevant Acts and regulations. The team is also implementing coordination mechanisms to ensure that its legislative and policy interpretation is consistent with other AML/ATF supervisory agencies, to the extent deemed appropriate given the nature and scope of the sector.

Back to Table of Contents

Reporting Entity Assistance

The development and circulation of Guidance Notes, as noted above, has been a key initiative in this regard. In addition, a number of outreach sessions have been held and an agreed strategy and action plan has been implemented to ensure that there is an ongoing programme to build awareness and understanding of AML/ATF matters, including in relation to ML/TF risks.

Risk-Based Monitoring and Inspection Programme

The team has completed its desk-based review of brokers' AML/ATF policies and procedures and has begun the implementation of its on-site inspection programme. The results of these reviews will be used to address issues of non-compliance, identify compliance trends and allow for the development and implementation of strategies to address common deficiencies.

Enforcement of Compliance

The SoRE has developed policies and procedures to promote and enforce compliance and intends to conduct annual reviews of the impact of corrective action to enhance the supervisory programme.

The Superintendent of Real Estate also has the goal of strengthening stakeholder relationships by actively participating in the AML/ATF Supervisory Forum (with other supervisory agencies) and the NAMLC Operational Working Group; and by collaborating with the Bermuda Chamber of Commerce – Real Estate Division on outreach to industry.

The Barristers and Accountants AML/ATF Board's Supervisory Approach

Outreach and Training

Outreach and training are key activities for the supervisory programme of the Board. Following the designation of the Board as the supervisory authority for entities in the legal and accounting sector, Guidance Notes and an Information Bulletin were developed for each sector and published in 2012 and 2018 respectively, with training and outreach delivered to the sectors thereafter. The Guidance Notes have since been updated, to reflect changes in the AML/ATF regulatory requirements and best practice. Training and outreach to RPFs and to the professional community in these sectors continue to be held on an ongoing basis to ensure that the knowledge and understanding of AML/ATF matters are continually strengthened. Information relating to the national and sectoral risks has been disseminated to allow for more effective risk analysis by regulated entities.

Back to Table of Contents

Oversight and Supervision

To ensure that entities complied with the requirements to register, discussions were held with firms regarding the nature and scope of their activities. RPFs were required to provide their policy and procedures manuals, and about their activities and the nature of their businesses.

The Board then conducted desk-based reviews involving analysis of the requested information, which was then used as the basis for onsite reviews on all the RPFs. Prioritisation of these inspections was done on the basis of the deemed risks arising from the desk-based review. The result of these inspections was a programme of remediation and ongoing monitoring to address issues of non-compliance. The Board has developed an enforcement plan, but to date no action has been deemed necessary, as firms have been responsive to taking the required actions based on the identified gaps. Work is currently ongoing to enhance the risk-based approach to supervision.

Legislation and Guidance

As noted previously, Guidance Notes and an Information Bulletin were issued for the Legal and Accounting sectors in 2012 and 2018 respectively. This guidance within both documents has been subject to comprehensive review and updating, in line with changes in the legislative framework.

The Board continues to review its legislative framework and to recommend changes to enhance it. The work currently being done in this regard will allow for more effective assessment of activities being undertaken by all firms, will strengthen the entry controls and will provide a wider range of sanctions that can be applied for non compliance.

Liaison with Other Relevant Bodies

Given the concurrent supervision of the Board in relation to RPFs and the BMA in relation to CSPs and TSPs in common ownership with such RPFs, the Board and the BMA have signed a Memorandum of Understanding (MoU) in relation to formalising an effective relation for cooperation and collaboration. Protocols in relation to that MoU are also being developed to ensure appropriate, entity-risk-specific group internal controls, with the standard to be applied where an RPF works jointly with its affiliated CSP or TSP.

The Board meets with the Bar Council and CPA to hold informational meetings, to distribute important announcements and documents and to communicate disciplinary concerns. There is also ongoing and positive communication with the oversight committees of these entities in relation to proposed legislative and framework changes which require the support of the sponsoring agencies.

Back to Table of Contents

Risk Assessment

The Board has also taken steps to strengthen its understanding and assessment of the nature, scope and risk of the business undertaken by the regulated sectors through data calls involving details which include:

- the risks of the firm
- the nature of the business
- clients
- transaction amounts
- services provided
- geographical details of the clients

In addition, the Board has reviewed the respective risk-assessments supplied by the RPFs. The analysis of the risk assessments is considered to be a vital component of the supervisory regime, in keeping with a risk-based compliance programme.

Oversight of Charities

Consistent with FATF requirements, the primary focus in relation to charities is their potential abuse as a mechanism for the financing of terrorism. An updated framework for oversight of charities was introduced in 2014 to bring the requirements for and oversight of Bermuda's charitable sector into compliance with FATF standards. The Act appointed the Registrar General as the supervisory authority for charities, as well as imposed a registration framework for charities to ensure compliance with the AML/ATF regulations. The framework was amended in 2016 in response to updates in the FATF standards.

Outreach and Training

The Registry General has issued Guidance Notes for charities on compliance with the AML/ATF Regulations, which are available online on the Government of Bermuda website. Also, the Registry General conducts training for charities' compliance officers on a quarterly basis, which is designed to enhance the sector's knowledge and understanding of AML/ATF matters.

Risk Assessment

A desktop review was conducted at the end of 2017 to evaluate the risk profile of registered charities. The criteria used for assessing charities' risk profiles included:

- the charities' volume of activities
- international/cross-border activities (foreign sources of funding or where a charity had overseas branches, or was itself a branch of an overseas entity)
- exposure to countries and regions that are vulnerable to terrorism (including, but not limited to, terrorism known to be associated with religious extremism)

These factors were used to create a risk matrix for assigning a risk profile to every registered charity. The Registry General began conducting risk reviews of registered charities commencing in July 2018, to identify trends in the charitable sector using the same criteria as the 2017 desktop review and a risk rating was assigned to all charities.

Back to Table of Contents

The Registry General has continued with its annual risk assessment of registered charities. Each charity is assessed when it submits its Annual Report and Financial Statements each year, and its risk profile/rating is reviewed. Charities deemed high risk are subject to additional review that take the form of desk-based and onsite reviews, followed by recommendations for addressing any identified deficiencies.

Oversight and Monitoring

The Registry General has implemented a supervisory programme for charities, consistent with its ML/TF risk. High risk charities are now subject to on-site visits to assess compliance with the requirements, which are intended to be conducted on a regular basis.

Addressing Non-Compliance

At the end of 2017, the Registry General commenced a compliance review of all registered charities to identify non-compliant charities so that appropriate action can be taken. As a result of the compliance review, several charities that were dormant have deregistered, and it is anticipated that several more charities may be forced to close as a consequence. Also, civil penalties have been imposed on five charities for non-compliance (failure to submit annual reports and financial statements within the specified timeline).

Since 2017, the Registry General has continued with its annual review of non-compliant charities to address the reasons for non-compliance and take appropriate action. As a result, the Registry General has been able to reduce the number of non-compliant/delinquent charities. Several charities have taken the appropriate action required in order to bring their respective organisations into compliance, whilst others were deregistered. The Registry General also continues to impose civil penalties on charities who fail to submit their annual report and financial statements within the specified timeframe, and on those charities who fail to report changes to their particulars within the prescribed timeframe.

B. Transparency and Beneficial Ownership

Bermuda has a long-standing beneficial ownership framework that requires all legal persons to be registered in the company registry and regulated financial institutions to have their beneficial owners (based primarily on voting shares) vetted by the BMA. This control mechanism has allowed for a focus on quality of applicants; therefore, Bermuda has approximately 16,000 registered companies.

Progressive enhancements to Bermuda's comprehensive beneficial ownership framework have led to the jurisdiction being recognised as a leader in this area. Since the last NRA exercise in 2017, Bermuda has enacted a suite of legislative amendments and key operational changes to enhance the effectiveness of its beneficial ownership regime and arrangements related to legal persons.

Back to Table of Contents

The fundamental change with respect to legal persons has been the introduction of a beneficial ownership regime under the Companies Act (and related Acts for the legal persons permitted in Bermuda, including LLCs and partnerships). This change complements the existing Exchange Control regime, to provide comprehensive coverage for all legal persons in line with the FATF standards. Bermuda has also adopted a definition of beneficial ownership compliant with the FATF standards, applied it uniformly to all types of legal persons and introduced obligations related to accuracy and timeliness of updates of beneficial ownership information. It also established a central register of beneficial ownership. In addition, all Corporate Service Providers are now licensed and regulated, and the regime introduced enforcement powers for the ROC. For legal arrangements, additional amendments to the Trustee Act ensure that all Trustees hold required information and that there are appropriate penalties in place for non-professional and exempted Trustees.

As a result of these changes, key components of the regime now include:

1. A central, comprehensive regulatory regime for obtaining and holding beneficial ownership information for legal persons, with consistent filing requirements. Complementing the legislative changes, the BMA has implemented a new system for recording information related to the beneficial ownership regime, the Exchange Control regime and the Regulatory regimes. This system supports electronic filings by companies for incorporation, exchange control permissions and changes of beneficial owners.
2. An appropriate enforcement framework and the ROC's compliance unit, which has and continues to conduct compliance and enforcement activity related to the beneficial ownership regime. The BMA has also established an Exchange Control compliance regime. The BMA and the RoC apply continual liaison and active collaboration to achieve the goal of effective and efficient supervision.
3. Corporate Service Providers are now all licensed by the BMA. This strengthens the overall CDD regime, as legal persons using the services of a CSP are subject to the CDD obligations of the CSP.

The BMA vets changes in beneficial ownership of all regulated financial institutions and most other legal persons with foreign ownership who represent more than two-thirds of registered persons. Shareholders and controllers of all regulated financial institutions are required to file and appropriately update beneficial ownership information with the BMA, which the BMA monitors. This includes information about controllers as per the FATF definition of beneficial owners. Additionally, all regulated institutions must carry out customer due diligence on all beneficial owners of their clients. This covers a high percentage of the entities formed in Bermuda, including legal arrangements. This information must be retained by regulated entities.

In the area of tax transparency, Bermuda was assessed and rated largely compliant overall under the Tax Transparency and Information Exchange Peer Review Assessment that was concluded by the Organisation for Economic Co-operation and Development (OECD) in 2017. The OECD conducts peer reviews of its member jurisdictions' ability to

Back to Table of Contents

cooperate with other tax administrations. Effective exchange of information requires that jurisdictions ensure information is available, that it can be obtained by the tax authorities and that there are mechanisms in place allowing for exchange of that information. The Assessment report indicated that Bermuda exchanged different types of information (ownership, accounting, insurance and banking), including information held in a fiduciary capacity during the period under review. It was also concluded that there were no limitations found in Bermuda's instruments and peers had not raised any issues in this respect. This highlights that Bermuda is recognised as having a strong framework in relation to tax transparency.

Consistent with our commitment to being a leader in relation to international agreements for exchange of information for tax purposes, Bermuda has undertaken the following:

- joined the OECD Inclusive Framework on Base Erosion and Profit Shifting (BEPS);
- implemented the OECD Country-by-Country (CBC) automatic exchange of information regime by collecting from Multinational Enterprises headquartered in Bermuda their 2016 fiscal year information by December 31, 2017 to exchange with CBC partner countries by June 2018; and
- signed a bilateral CBC automatic exchange of information competent authority agreement with the United Kingdom of Great Britain and Northern Ireland and the USA

  Bermuda also became an early adopter to automatically exchange the OECD Common Reporting Standard (CRS) information; and was among the countries that signed the multilateral competent authority agreement (MCAA) for CRS in Berlin in October 2014 and subsequently exchanged 2016 year CRS information.

Bermuda has also signed more than 40 bilateral Tax Information Exchange Agreements (TIEAs) and has joined the Joint Council of Europe-OECD Multilateral Convention on Mutual Administrative Assistance in Tax Matters (the Convention), in which Bermuda's participation entered into force and effect on March 1, 2014. This agreement immediately established a tax information exchange relationship with more than 110 countries.

Bermuda's total portfolio of approximately 16,000 registered legal entities highlights the ongoing commitment that has been made to attracting quality over quantity and this—coupled with the demonstrated commitment to transparency—reinforces the objective that Bermuda will continually strive to be a good place to do good business.

Finally, Bermuda has more recently reflected its policy of adherence to agreed emerging international tax standards. This was documented by filing with the OECD, Bermuda's agreement to "The October 8th, 2021, G20/OECD Statement on the Two Pillar Solution" issued by the OECD's committee known as The Inclusive Framework on BEPS.[6]

[6] BEPS means Base Erosion and Profit Shifting

Back to Table of Contents

C. International Cooperation

The Government of Bermuda is committed to cooperating with other countries and with regional and international organisations to combat ML/TF. Bermuda's relevant authorities have, as appropriate, developed strong links with their international counterparts and are active in regional and international bodies, where AML/ATF matters are addressed. Gateway provisions in the required legislation ensure that information can be appropriately shared with counterparts in other jurisdictions.

Through the Mutual Legal Assistance Treaty (MLAT) process and the various tax treaties and agreements that Bermuda has become a signatory to, Bermuda is able to both provide and request information to assist or gain assistance from overseas authorities in investigations and even, through appropriate mechanisms, in the prosecution of relevant crimes.

Through the extensive network of financial intelligence units that are part of the Egmont Group, the FIA is actively involved in exchanging financial intelligence. In addition, through relationships within the Caribbean Action Task Force (CFATF) and other such bodies, the FIA is able to have and use information-sharing agreements with non-Egmont FIUs. The BPS interacts on a regular basis with foreign law enforcement agencies, including the UK's National Crime Agency, the FBI and other such bodies. Customs cooperates with all customs counterparts world-wide through the World Customs Organization (WCO) and regionally through the Caribbean Customs Law Enforcement Council (CCLEC). They also work closely with the following: the United States Customs Border Protection, which has a pre clearance unit in Bermuda; the Canada Border Services Agency Liaison Officer, who is stationed in New York and meets with Bermuda on a regular basis; and the UK Border Force; and the National Crime Agency (NCA). Agreement has now been reached for the Regional Intelligence Liaison Officer (RILO) post for CCLEC to operate out of Bermuda. The RILO works closely with Bermuda's Joint Intelligence Unit as well as the regional Caribbean Customs Departments to communicate and disseminate all aspects of intelligence through the CCLEC Organisation.

The sectors supervised by the BMA have a significant impact on Bermuda's economy. The BMA is actively involved in international standard-setting bodies such as the International Association of Insurance Supervisors (IAIS), the International Organization of Securities Commissions (IOSCO), and the Group of International Financial Centre Supervisors (GIFCS) as well as having strong links with supervisory bodies in key financial centres such as the United States' Securities and Exchange Commission (SEC), the UK's Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA) and the European Insurance and Occupational Pensions Authority (EIOPA). The BMA hosts or attends supervisory colleges in relation to the oversight of entities that have global operations. Through this and other mechanisms, the BMA and other supervisors as appropriate ensure that there is coordinated engagement, where necessary, to strengthen the effectiveness of the regulatory and AML/ATF framework, from a domestic and international perspective.

Bermuda is actively involved in the Caribbean Action Task Force (CFATF) and, through membership in that body, has been able to play a role even in FATF matters. In this regard, Bermuda chaired a joint CFATF/FATF typology report on Money Laundering Using Trust and Company Service Providers, which was published in October 2010. Bermuda will continue its strong and active support of global and regional initiatives in the fight against ML, TF and PF activities.

Chapter 4: Methodology for the Money Laundering Risk Assessment

Introduction

In accordance with the National AML/ATF Policy, NAMLC is responsible for ensuring that competent authorities collaborate to keep Bermuda's understanding of its ML risk up-to-date. NAMLC also develops and proposes to Cabinet any policies or strategies that are geared toward mitigating the identified risks. On that basis, in 2020 NAMLC conducted Bermuda's third Money Laundering National Risk Assessment (ML NRA).

The Methodology

The 2020 National Risk Assessment on Money Laundering (the 2020 ML NRA) began in November 2020 and was led by NAMLC, with the support and sanction of the Cabinet and Public Service Executive. The Office of NAMLC, which provides secretariat services to the Committee, coordinated the entire project. One (1) dedicated coordinator was temporarily reassigned to the Office from another Government department to manage the NRA; and an international AML expert was engaged as a Consultant, to provide technical guidance and support throughout the project to the participating NAMLC agencies and to the Chairs of all working groups.

As with previous Bermuda NRAs, the methodology used for this NRA is premised on the concept of ML risk being a function of money laundering threats and vulnerabilities. An ML risk assessment is a process that attempts to identify, analyse and understand ML risks and serves as a first step in addressing them. Ideally, an ML NRA involves making judgments about the criminal threats to which the country is exposed and vulnerabilities that could be exploited by criminals. These key concepts are explained by the FATF[7] as follows:

a. **Money Laundering**: The process used by criminals to conceal or disguise the origin of criminal proceeds to make them appear as if they originated from legitimate sources.

b. **Threats**: These are the predicate crimes that are associated with money laundering. In some cases, specific crimes are associated with specific money laundering methods. In any event, crimes and criminal activity which generate proceeds that can be laundered make up the threat environment. Understanding the threat environment is essential to understanding the vulnerabilities that create money laundering opportunities, and to understanding the residual risks.

c. **Vulnerability**: This comprises those things that can be exploited by the threat or that may support or facilitate its activities. Vulnerabilities facilitate or create the opportunity for money laundering. They are weaknesses inherent in a specific financial sector or product; or a weakness in the laws; or in the regulation, supervision, or enforcement framework; or may reflect unique circumstances in which it may be difficult to distinguish legal from illegal activity.

[7] FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment, February 2013

Back to Table of Contents

d. **Consequence**: refers to the impact or harm that ML may cause and includes the effect of the underlying criminal activity on financial systems and institutions, as well as the economy and society more generally. The consequences of money laundering may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector.

Given the challenges in determining or estimating the consequences of ML, the FATF allows for countries to focus their risk assessment efforts primarily on achieving a comprehensive understanding of their money laundering threats, and vulnerabilities.

The Risk Assessment Tool

The 2020 assessment used the World Bank risk assessment model, allowing for continuity and comparability, since this tool was also used in the 2013 and 2017 ML NRAs. Although the tool used in 2017 was more or less identical to the version used in 2020, the tool did undergo fairly comprehensive updates between the 2013 and 2017 iterations, as the World Bank incorporated feedback from users around the globe. However, it should be noted that although the tool used was designed by them, the World Bank took no part in Bermuda's 2020 ML NRA and they provided no technical input nor guidance in either the analysis conducted or the conclusions drawn.

The 2020 assessment was conducted using the World Bank Model's seven (7) ML modules, namely:

MODULE 1 National Money Laundering Threat;

MODULE 2 National Vulnerability;

MODULE 3 Deposit-Taking (Banking/Credit Union) Sector Vulnerability;

MODULE 4 Securities Sector Vulnerability;

MODULE 5 Insurance Sector Vulnerability;

MODULE 6 Other Financial Sectors Vulnerability – namely, Money Service Business, Lending and the Stock Exchange, and;

MODULE 7 Non-Financial Sectors Vulnerability – namely Designated Non-Financial Businesses and Professions (DNFBPs) and others, that is:

- Trust Service Providers;
- Corporate Service Providers;
- Casino Gaming;
- Real estate dealers;
- Lawyers;
- Accountants;
- Dealers in Precious Metals and Stones;
- Other Dealers in high value goods – cars, boats, bikes, antique dealers and auctioneers; and
- Betting shops.

Back to Table of Contents

Module 1 evaluates national ML threats; the Working Group used this Module to determine a subjective ranking of the ML threats from the various predicate offences. The module also requires ranking of ML threats to each sector, as well as the identification and ranking of cross-border threats.

Modules 2 - 7 are applied for the vulnerability assessment, examining key features of the national or sectoral AML/ATF framework, or the products each sector offers; the Working Group assigned a quantitative rating to each sector and product assessed, and the ratings were ultimately translated by the tool into the respective vulnerability ratings.

More information about the World Bank Tool is provided in Appendix B.

The Scope

Financial and Non-Financial Sectors

The 2020 ML NRA focused solely on assessing Bermuda's money laundering risk and was conducted as a follow-up to the 2017 NRA on money laundering. The agreed review period was from 1 January 2017 through to 31 December 2019, though material changes to the legislative or institutional framework which came into effect in 2020 were taken into account where appropriate.

As was the case in 2017, the 2020 ML NRA examined the financial and non-financial sectors relevant to AML regulation and oversight, i.e. Deposit-Taking (Banking & Credit Union), Securities, Insurance, Money Service Business, the newly brought into scope Lending sector, the Bermuda Stock Exchange, Trust and Corporate Services Providers, the Legal and Accounting professions, Real Estate Brokers, Dealers in Precious Metals and Stones, Dealers in High Value Goods[8], the Betting sector[9] and the Casino Gaming sector, even though there are still no casino operations functioning in Bermuda. Each responsible supervisory authority conducted the vulnerability assessments for their respective sector, with direct or indirect input from the regulated sectors. The input and participation of the Betting Licensing Authority[10] (which was then responsible for the Betting Sector) was also sought, even though this sector is not subject to AML supervision or oversight.

[8] Dealers in cars, boats, trucks and motorbikes.

[9] It should be noted that the betting sector is not subject to AML/ATF obligations or supervision.

[10] On 1st August 2021, the Betting Act 2021 became operational and designated the Bermuda Gaming Commission as the authority responsible for the licensing and supervision of betting operations.

Back to Table of Contents

Digital Asset Business and Legal Persons

Although regulatory frameworks were developed for the Digital Asset Business sector and for Digital Asset Issuance in 2018 and 2020 respectively; this activity and the regulated sector were not included in the scope of this national assessment. This is because a focused assessment of both regulated and unregulated digital asset-related activities is planned to follow the conclusion of this NRA, using a bespoke tool developed for this purpose by the World Bank. This tool requires an holistic assessment of both the vulnerabilities and the threats unique to digital assets in order to determine the ML/TF risk. Therefore, Bermuda and the BMA as the supervisor of regulated Bermuda digital asset businesses, will benefit from having a targeted assessment, focused on the unique features of the sector's products and services. NAMLC has agreed that following the assessment of this sector, the resulting report will be appended to the published consolidated ML/TF NRA report when it is completed.

The assessment of vulnerabilities of the various types of legal persons that can be formed in Bermuda was also not included in the scope of this NRA. A standalone risk assessment of legal persons continues to be a requirement of the National AML/ATF Policy and an updated assessment is already underway, utilising a bespoke risk assessment tool for Legal Persons which has been developed by the World Bank. NAMLC has agreed that upon completion of this assessment, the resulting report will be appended to the published consolidated ML/TF NRA report when it is completed.

The Working Groups

A separate Working Group was established to carry out the assessment required by Modules 1 and 2 respectively and for each of the sectoral assessments conducted using Modules 3 – 7. The Working Groups comprised representatives from all relevant national competent authorities with responsibility for AML matters, including law enforcement, financial intelligence, prosecutors, supervisory authorities, the tax authority, company registry, and the agencies responsible for mutual legal assistance, civil asset recovery, tax information exchange, customs/border control/immigration control; and also including the national coordinating agency. For all sectoral assessments, the Working Groups were chaired by the relevant supervisory authority for each sector being assessed.

A list of the individual Working Groups is provided in Appendix C.

As noted above, each sectoral Working Group assessed the money laundering vulnerabilities of their sector, using Modules 3 – 7, as was relevant to the sector in question. These assessments examined both the inherent ML vulnerability factors specific to each sector, as well as the effectiveness of the mitigation measures in place within the sectors and at supervisory level.

The National Threats Working Group focused on evaluating criminal activity that occurs both locally and overseas that can give rise to money laundering in Bermuda, using Module 1. This involved assessing predicate crimes that generate criminal proceeds and contribute to ML in Bermuda; iden-

Back to Table of Contents

tifying and ranking the sources of ML threats; analysing the sectoral threats; and determining the nature and direction of the cross-border ML threats vis-à-vis a select group of countries based on their economic and crimino-legal connections with Bermuda. The sectoral Working Groups were also provided with threat rankings by sector, so that they could determine sectoral ML risk ratings.

The National Vulnerabilities Working Group used Module 2 and focused on assessing the nature and effectiveness of the AML/ATF laws, institutional framework, policies and strategies, to determine the national ML combatting ability. This assessment also synthesised the outputs from all of the sectoral assessments. However, in this report, only the findings related to inherent vulnerabilities within each sector are provided, along with the findings on ML threats. These factors constitute the inherent risk findings. Comprehensive information on the effectiveness of Bermuda's AML/ATF framework is available in Bermuda's 2020 Mutual Evaluation Report[11].

Post-Analytical Validation Workshops

The preliminary findings of all the Working Groups as well as their recommendations for next steps were presented to broader national stakeholder groups – both private and public sector, composed of competent authorities, government executives, and industry representatives, in a series of virtual workshops. Feedback from these workshops helped to refine the Working Groups' findings further.

[11] Published on the FATF's website: https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/CFATF-Mutual-Evaluation-Report-Bermuda-2020.pdf

Back to Table of Contents

Chapter 5: Bermuda's National ML Threats

Introduction

In the 2017 ML NRA, it was reported that Bermuda boasts a relatively low crime rate, a high standard of living and high respect for law and order amongst the majority of its resident population. This assessment remains largely unchanged, however, unlike in the previous ML NRA when the 10-year downward trend in crime statistics continued in that review period, from 2017 to 2019 the Bermuda Police Service reported an increase in crime categories. The table below compares the crime statistics for the 3-year review periods for the 2017 and 2020 ML NRAs.

Table 3: Comparative Crime Statistics for the 3-Year Review Periods for the 2017 and 2020 ML NRAs

BPS Crime Categories	2014-2016	2017-2019
Crimes Against Property	5,332	6,659
Crimes Against the Community	1,114	1,511
Crimes Against the Person	1,848	2,127
Drug Enforcement	1,076	1,441
Total	**9,370**	**11,738**

Grave offences such as murder for hire, kidnapping or other serious offences against the person, done for financial reward, still do not feature in Bermuda. In addition, law enforcement continues to note that the vast majority of crimes against property reported to the Police are of low financial value, and are associated with violence against individuals very rarely. It is estimated that the average value of loss for such crimes still remains in the region of $5,000.

While drug trafficking occurs in Bermuda and is profitable, Bermuda is seen as an 'end destination' rather than as a 'production' or 'transshipment' locale for drug trafficking, due in large part to its geographic location. Additionally, its high standard of living is what makes the reward for drug trafficking in Bermuda a highly profitable crime, even though the market is small and finite. As it is not a transshipment destination, Bermuda is spared much of the criminality associated with highly organised crime syndicates, which is often seen in jurisdictions that participate in drug production and drug transshipment.

The Bermuda Police Service and the Department of Public Prosecutions are the national investigative and prosecuting authorities. Investigation and prosecution of criminals for crimes either reported to or detected by the Police Service are the remit of these two authorities. The results of criminal cases are routinely reported in local print and digital media, making the administration of justice and functioning of the Courts in Bermuda, from the lowest to the highest, highly visible. This visibility of the law at work contributes to the high degree of respect for law and order which is the norm in Bermuda.

Back to Table of Contents

Scope and Process

The National Threats Working Group assessed Bermuda's national ML threat profile. This group comprised representatives from relevant competent authorities covering law enforcement, prosecutorial, tax and AML supervision and enforcement in the financial sector. Additional support and relevant data was provided by the Department of Statistics and the Department of Immigration.

The assessment considered the amount of proceeds of crime that criminals could potentially launder through Bermuda's financial and non-financial sectors. Achieving that goal is impeded at the global level, due to limited knowledge of the criminal environment which arises from imperfect rates of detection of crime, and the inherently secretive nature of criminal activity. Taking these factors into account, the analysis involved estimating and understanding, in monetary terms or with qualitative data, the value criminals gain from and through crime in Bermuda. This analysis also estimated the value of proceeds of crime exported to Bermuda from abroad, and an estimate of possible undetected criminal proceeds.

The following key factors were considered:

- criminal offences in Bermuda and overseas which generate proceeds that can be laundered in Bermuda (the 'predicate offences');
- the number of incidences of each of the predicate offences; and
- the average value generated by an individual offence.

Each predicate offence was assessed using a 5-level 'money laundering threat' ranking of LOW, MEDIUM LOW, MEDIUM, MEDIUM HIGH or HIGH. In engaging in this process, consideration was given to the sources of data and information that was available; as well as the key limitations of the data and possible means to address any shortcomings.

In order to rank the money laundering threat, benchmarks were set to have consistency of ranking across all sectors. After a review to determine any potential necessary updates, the original benchmarks from the 2017 ML NRA were used for the 2020 analysis, and were based on the estimated proceeds of crime generated by domestic crime. Generally, domestic crime was rated as a lower threat, recognising that international proceeds of crime laundered in Bermuda will typically be larger in scale and consequently will be rated as higher-threat.

The selected benchmarks were adhered to when analysing threats associated with predicate offences, sectoral threats, and the origin of ML threats. However, when assessing cross-border threats and coming to conclusions on the overall threat results, a broader approach was taken. This approach took account of the sheer scale of economic activity in international business, which significantly outpaces the size of domestic economic activity, thereby giving appropriate weight to the potential for substantial difference between domestic and foreign sourced proceeds. The 2020 ML NRA benchmarks are listed below, with the figures applicable to the full 3-year period under review (i.e. not per annum):

Back to Table of Contents

High	+$10million
Medium High	+$1million
Medium	+$100,000
Medium Low	+$50,000
Low	under $50,000

The full range of predicate offences as required by FATF were considered in this assessment, taking into account the peculiarities of Bermuda's criminal laws and other national realities, resulting in a total of 25 predicates. Data was gathered from all relevant agencies and covered the following areas, among others:

- the number of cases detected/investigated and prosecuted for each predicate and for money laundering;
- the number of financial intelligence disseminations provided to law enforcement and foreign counterparts;
- the value of property seized or frozen and the value of property confiscated through criminal or civil processes; and
- the number and nature of international cooperation requests received from or sent to foreign counterparts.

The review period used during this NRA, for the purposes of data collection was 1 January 2017 to 31 December 2019. However, qualitative information about cases and interactions that occurred since the end of this review period were also considered and factored into the analysis, where appropriate. The data collected was considered from different perspectives in all aspects of the ML Threats assessment, namely for rating predicate offences, as well as of the origin of the crimes, the sectoral threats and the cross-border threats. Analysing data from these varying perspectives showed whether the source of Bermuda's money laundering threat is international, domestic or a mix of the two. The sectoral analysis showed which sectors in the economy are either most impacted by ML threats, or play the most pivotal roles in money laundering in Bermuda.

For the cross-border threat analysis, 12 countries were identified and assessed, as they featured most prominently or frequently in trade in goods and services with Bermuda, foreign investment, cross-border aspects of criminal cases, tax information exchange requests or other international cooperation in criminal matters. Data from the relevant agencies, along with economic data from the Department of Statistics and the Bermuda Monetary Authority, was also analysed to gain a better understanding about the international nature, scope and direction of ML threats.

Back to Table of Contents

Predicate Offences Generating Proceeds of Crime

Analysis of the data and cases determined that predicate offences posing the HIGHEST threat of money laundering to Bermuda primarily originate from overseas and are Fraud, Corruption/Bribery, Insider Trading/Market Manipulation and International Tax Crimes. Domestically, Trafficking in Narcotics remains the highest ML threat, followed by Corruption/Bribery. These ratings are consistent with the findings in the 2017 NRA.

Data was gathered about 25 predicate offences of money laundering. Aside from the predicates rated as High, the only other predicate offence of note was Domestic Tax Crime, which was rated at MEDIUM threat for money laundering. Unlike in 2017, there were no predicates rated as Medium-High. Two (2) offences were rated as Medium-Low, namely Illicit Arms Trafficking and Commercial Smuggling; and the other thirteen (13) predicates were rated as representing a low threat for money laundering in Bermuda. Unlike in 2017, the threat of money laundering from unspecified predicate offences was rated as Low, as in the vast majority of money laundering cases in Bermuda, authorities were able to readily identify the underlying criminality that generated the laundered proceeds.

I. Predicate Crimes Ranked as HIGH THREAT

These findings were based on statistical evidence of cases investigated and prosecuted for those crimes, and on the value of proceeds generated based on the amount of proceeds confiscated. However, part of the assessment included the estimated value of undetected proceeds from those crimes, based on law enforcement's understanding of crime detection levels, or on other indicators which support the conclusions.

i. Fraud

As in 2017, the offences of fraud, forgery, deception and counterfeiting currency were all considered within this category of offence, as the data for each of these offences could not be disaggregated. The Police Service continues to record composite statistics covering a broad range of deception-based offences under the Criminal Code 1907. The law enforcement and prosecutorial experience in most domestic cases of fraud during the review period was that they were generally of low value, averaging $5000 or less. The Police detected or investigated 383 instances of these offences, resulting in 19 prosecutions and 11 convictions. Approximately $174,000 was restrained or seized in relation to this predicate, resulting in approximately $95,000 in confiscated proceeds.

Back to Table of Contents

In relation to domestic fraud, although the overall number of frauds reported had reduced by almost 20% compared to the previous period, during the 2020 assessment there were a fairly large number of domestic fraud investigations that involved money laundering. During this review period 40 ML cases were investigated, resulting in 4 ML prosecutions and 3 convictions. However, it was noted that none of these investigations or prosecutions involved any seized or restrained proceeds, and there were no confiscations or forfeitures associated with these cases.

Law enforcement noted this was partly due to an increase in cyber-based fraud. Although there was a large amount of these types of fraud cases, they have low monetary gain and the ML associated with them involves local victims transferring funds overseas to locations specified by the offenders. These cyber-crimes include credit-card harvesting or phishing (namely, providing victims with false links to their bank's website, thus enabling predators to harvest their account's login information), as well as ransom-ware targeted at businesses in a few cases. Even in those cases, the ransom demands reported have been in the range of $500-$600 demanded in crypto currency, though the businesses have not usually actually made such payments.

Another reason for the ML investigations relates to another emerging type of fraud known as elder abuse, involving the targeting and misappropriation of funds belonging to vulnerable elderly persons. Given the emerging social concern about this preying on a vulnerable population, there has been significant work done by local charities as well as public education initiatives supported by law enforcement, the banking sector and the Ministry of Health, which has led to marked improvement in detection and reporting rates for this crime.

Given these developments, it was difficult to ascertain the level of undetected proceeds from domestic frauds. This is particularly so in relation to the cyber-based frauds, as local victims of these crimes might not be motivated to report them because of the low dollar values involved, the belief that the suspects overseas are hard to trace from their online persona, and because of personal embarrassment. Elder abuse fraud is also quite dependent on financial institutions noticing patterns and reporting SARs, or community members with information reporting to the Police, as the victims may not be able to do so. In relation to the more traditional types of frauds, law enforcement is of the view that these enjoy a very high level of reporting, due to the strong demand for justice in such matters, even where the amounts defrauded are low.

For money laundering derived from frauds committed overseas, there were more mutual legal assistance and civil asset recovery cases, with higher values, when compared to 2017. The Central Authority received 19 mutual legal assistance requests in relation to overseas ML and fraud investigations and prosecutions. In one of these cases,

Back to Table of Contents

the Central Authority secured a restraint order for funds totaling over $1.9 million on behalf of foreign counterparts. However, this Order eventually had to be discharged due to lack of forthcoming evidence from the requesting country, to justify continued restraint of those funds. There were also three domestic Civil Asset Recovery cases arising from ML associated with fraud during the same period, resulting in over $13 million being frozen. None of the civil asset recovery matters involved any proceeds from domestic fraud. Although there were no confiscations associated with these civil asset recovery cases during the review period, this was because they were all still pending at the time of the NRA, so no final orders for confiscation had been made.

The exchange of financial intelligence related to this predicate is another relevant indicator. The FIA received 13 incoming requests from foreign FIUs, and assisted with identifying accounts and assets pertinent to fraud inquiries underway overseas. The FIA also made 33 outgoing requests relating to suspected foreign fraud. The predicates in these incoming and outgoing requests were associated with 27 countries; and the policies and products in Bermuda identified as receiving funds associated with some of these inquiries, were opened with funds originating from foreign accounts.

Considering these factors, Fraud was again ranked as representing a HIGH threat of money laundering in Bermuda, retaining the 2017 rating. It was also confirmed that proceeds derived from fraud committed overseas remained the more substantial source of ML, compared with domestic fraud (more accurately dual jurisdictional fraud), where local victims unwittingly participate in the laundering of the defrauded amounts, but in which the values involved are quite low. The proceeds from frauds committed overseas that make their way into Bermuda's financial system are of much higher value, as seen by the civil asset recovery and mutual legal assistance cases. These cases also demonstrate the various avenues used within Bermuda's financial system to launder those proceeds.

Other than Trafficking in Narcotics, the offence of Fraud is the only other predicate that has consistently rated high for ML threat since the 2013 ML NRA.

ii. Trafficking in Narcotics

Consistent with the approach in 2017, all offences under the Misuse of Drugs Act 1972 were considered, covering the retail drug trafficking offences that occur at street level, as well as wholesale drug trafficking offences, i.e. importation and conspiracy to import narcotics into Bermuda. The traditional context of drug trafficking in Bermuda remained unchanged: all drugs sold in Bermuda are imported from elsewhere, and it remains an end-user destination for drugs. This means that drugs landed in Bermuda are destined for the local market and not for repackaging and trans-shipment as in other jurisdictions in the region.[12] Further, Bermuda is not a producer of drugs for domestic consumption.

[12] As was done in 2017 (for the first time), this category of offences is to be distinguished from the Transit in Narcotics predicate, which is considered separately from the drug trafficking offences. Transit covers the drugs that are onboard vessels that transit through Bermuda's ports, without being landed in Bermuda.

Back to Table of Contents

Importantly, the street value of drugs in Bermuda is significantly higher than in other countries. As a result, there is generally a significant spread between the wholesale value of the drug at the point of purchase for importation and the retail value on its arrival in Bermuda. Unlike in 2017, there was no available information on the estimated annual average value of the drug market in Bermuda,[13] primarily because there were no street value assessments of the drugs seized in the 2017 to 2019 period. Law enforcement expressed the view that their drug trafficking detection rate[14] had not significantly changed during this review period. Related data showed that suspected proceeds were seized/restrained in only a few drug trafficking or related ML cases; proceeds were confiscated in only two ML cases that were based on drug trafficking.

Over the period 2017 – 2019, law enforcement detected 1020 drug trafficking cases,[15] resulting in 117 cases being prosecuted, with convictions resulting in 69 of those cases. Proceeds of crime confiscated or forfeited from drug trafficking cases, prosecutions and civil actions, amounted to approximately $350,000. Over $900,000 was restrained and forfeited in Bermuda as a result of mutual legal assistance requests received in relation to suspected drug trafficking.

During that same period, 25 money laundering cases were investigated where drug trafficking was the predicate, resulting in 14 cases being prosecuted, with convictions resulting in 10 of those cases. From one of these cases, approximately $176,000 was confiscated, representing the total amount of property originally seized or restrained in connection with all of the ML cases. Approximately $314,000 was also frozen under the civil asset recovery regime based on suspicions of drug trafficking and ML. This case was still pending at the time of the 2020 ML NRA.

The ML threat rating for drug trafficking therefore remained HIGH. Despite the decline in seized proceeds and the absence of data on street value of drugs, there is confidence that the demand for illicit drugs in Bermuda and the higher retail value of such drugs results in a fairly stable retail drug market.

[13] In 2017, information from BerDIN, confirmed by the Police, indicated that the annual average value of the drug market in Bermuda was approximately $25 million.

[14] The detection rate for drug trafficking was assessed as approximately 20% over previous review periods

[15] The 2020 BERDIN Annual Report indicated that due to decriminalisation in Bermuda of possession of less than 7.0 grams of cannabis, 2019 saw a significant reduction (22%) of cannabis seizures by BPS, compared to 2018.

Back to Table of Contents

iii. Corruption/Bribery

During the 2020 NRA review period 27 cases of corruption/bribery were detected or under investigation domestically, with 2 cases proceeding to prosecution and resulting in convictions. The BPS investigated 11 ML cases involving money laundering derived from domestic corruption/bribery, with two cases having been put before the courts. The FIA made 10 disseminations to the BPS relating to suspected corruption/bribery, six of which were primarily identified from disclosures/requests received from Egmont Group[16] counterparts concerning foreign individuals. The other four related to ongoing domestic investigations.

Unlike in 2017 there were no civil asset recovery actions related to this offence during the review period. However, international cooperation between Bermuda's FIA and foreign FIUs continued to be beneficial. Bermuda provided evidentiary or other legal assistance to foreign authorities in response to two MLA requests for corruption and one for bribery. In one of the MLA requests, the authorities restrained funds exceeding $40 million related to a foreign corruption investigation, where the alleged corruption occurred overseas. The FIA also received 12 incoming requests from foreign FIUs related to corruption/bribery, and made 10 outgoing requests. There were 13 countries identified as the origin of the corruption/bribery involved in these exchanges. It was also notable that the local accounts connected to these inquiries had been opened with suspected criminal proceeds originating from foreign accounts.

A number of domestic cases of suspected high-value corruption/bribery, as well as the three MLA requests received during the period, exceeded the "high threat" threshold of $10 million. Accordingly, it was determined that a **High** threat rating for corruption/bribery remains justified, based on the potential scale of proceeds derived from both domestic and foreign sources of this predicate.

iv. International Tax Crimes

During this review period, the Ministry of Finance reported receiving 93 criminal tax requests for information or evidence; while the Central Authority received 2 mutual legal assistance requests from foreign counterparts in respect of tax evasion investigations. In relation to the mutual legal assistance requests, local authorities have provided material investigative assistance and continue to provide legal support in these foreign investigations. Authorities in Bermuda have also restrained funds amounting to $55,000 in one of the MLA matters. There were no other funds seized or confiscated in relation to these matters. In terms of financial intelligence shared between the FIA and their foreign counterparts, the FIA assisted in the identification of accounts and assets in response to 11 incoming requests. On the other hand, based on SAR filings connected to this predicate, the FIA also made 23 outgoing requests. In total, there were 12 countries involved in these incoming and outgoing requests and exchanges of information.

[16] The Egmont Group of Financial Intelligence Units (FIU) is an international organization, which was created to provide FIUs around the world with a forum to exchange information confidentially to combat Money-Laundering, the Financing of Terrorism and other predicate offences.

Back to Table of Contents

Outside of the international cooperation matters, there have been no local investigations nor prosecutions for foreign tax crimes, nor any civil asset recovery matters arising from such foreign crimes.

When considering how to rank the ML threat from foreign tax crimes, the number of treaty requests received from foreign jurisdictions in accordance with Tax Information Exchange Agreements (TIEAs),[17] was taken into account. In accordance with confidentiality obligations within OECD and other tax information exchange frameworks, no details related to the requests were shared by the responsible Ministry, nor any information about the countries from which the requests came. The aggregate number of criminal requests made during the period under the TIEA framework was much higher than the amount reported during the 2017 ML NRA, at which time it was 8 requests – compared with 93 during this NRA. Given the likely value of criminality involved in these 93 tax requests, it was estimated that the undetected proceeds of foreign tax crimes in Bermuda would likely exceed $10,000,000.

Of greater significance in assessing the ML threat from foreign tax crimes, is the fact that one of the two MLA requests involved a substantial foreign investigation of tax evasion. In that case, only a small percentage of the estimated overall proceeds being investigated, was suspected to be connected with Bermuda. This small percentage amounted to more than $100 million.

In light of these factors, the ML Threat rating of HIGH for International Tax Crime was retained. Even though it was difficult to estimate the undetected proceeds of this crime during the review period, it was determined that the actual cases examined, as well as the significant increase in criminal tax requests received under the TIEA framework during this time, made this predicate one of the most significant ML threats to Bermuda for this review period.

v. International Market Manipulation/Insider Trading

The BMA received 25 requests from foreign regulators during the review period concerning ongoing criminal investigations in foreign jurisdictions for this predicate. There were 17 SARs filed with the FIA in relation to this offence, although the majority were related to the same subject or activity. The FIA also received 2 requests from Egmont Group counterparts about investigations that were underway overseas. As was the case in the 2017 ML NRA, confidentiality arrangements in place between the BMA and their counterparts for international cooperation requests meant that no information was provided about the value of proceeds involved in the cases.

[17] TIEAs are required by the OECD's Global Forum on Transparency and Exchange of Information for Tax Purposes

Back to Table of Contents

It was acknowledged that Bermuda's connection with the activities under investigation in those cases could have been limited. However, it was reasonable to conclude that given the number of cases involved, the value of proceeds in Bermuda from this predicate would very likely exceed the $10 million threshold. This view was further compounded since several of the SARs filed with the FIA were connected to subjects or activities from investigations in progress overseas.

Accordingly, International Market Manipulation/Insider Trading was rated HIGH for the threat of money laundering. This rating is the same as in 2017, with the rationale remaining generally the same, based on the estimate of proceeds in Bermuda exceeding the threshold for High. The fact that this predicate is foreign-based, and Bermuda's international financial services sectors are exposed to foreign clientele, compounds the potential threat from this crime.

II. Predicate Crimes Ranked as MEDIUM THREAT

Domestic Tax Crimes is the only predicate that has been rated as MEDIUM Threat for ML in the 2020 NRA. This rating is lower than the 2017 rating of medium-high. In determining the appropriate rating, it was considered that among the four investigations for fraudulent tax evasion in Bermuda during the review period, none involved ML. In 2017 the rationale for the Medium-High rating was based on the number and value of actions taken by the Office of the Tax Commissioner (OTC) to pursue delinquent taxpayers. At that time the OTC's priority was revenue recovery, not on distinguishing between delinquency and criminal tax evasion. Therefore, with over 40 debt collection cases pursued during that review period and with a debt portfolio of over $2.7 million, this was the determining factor for the 2017 rating.

The 2020 approach was to focus directly on the types of cases that are potential predicates for money laundering, as only a limited range of delinquent behaviour generates proceeds that can then be classed as criminal in origin and therefore laundered. Only fraudulent tax evasion of payroll tax and betting duty come within this category. This adjusted approach reflects the recommendation made after the 2017 ML NRA that the OTC and the BPS should develop protocols to identify and refer such cases to the BPS for investigation.

On that basis, data on a total of four such cases involving unpaid taxes totaling approximately $1.2 million and referred to the Police for investigation and prosecution were examined. Law enforcement concluded that the case with the largest value of unpaid taxes was not fraudulent in nature. Lack of evidence definitively proving fraudulent tax evasion meant that there were no prosecutions in the remaining three cases.

Given the lack of data and challenges in law enforcement and prosecutorial experience with these cases, it was difficult to determine the extent of the undetected

Back to Table of Contents

proceeds from this crime. However, it was determined that a lower rating compared with 2017 was appropriate given the nature of the cases, relatively low individual values involved, and the limited pattern observed. Those factors distinguish them from the majority of tax delinquency cases.

III. Predicate Crimes Ranked as MEDIUM–LOW THREAT

Commercial Smuggling and Illicit Arms Trafficking were the only predicates rated as MEDIUM-LOW in this NRA. This rating is consistent with 2017 regarding arms trafficking, and lower in the case of smuggling.

In relation to Illicit Arms Trafficking, there were 53 investigations of various firearms offences, the majority being unlawful possession and discharging of a firearm. There were nine prosecutions for various firearms offences, resulting in four convictions. While there were three ML investigations and two prosecutions which also involved firearms offences, there have been no convictions and at the time of the assessment one prosecution was still pending.

Additionally, there have been no funds/assets confiscated on the basis of being the proceeds of trafficking in arms. It was noted that in a few cases, firearms had been detected at a port, being imported in parts in multiple shipments; one case resulted in a conviction during the review period. Similarly, there have only been a few instances where ammunition arriving into Bermuda was detected and seized. It is accepted that the majority of firearms/ammunition unlawfully imported into and trafficked within Bermuda is not being detected and it is believed that the detection rate may be similar to that of narcotic imports, namely about 20%.

When compared with the 2017 findings the circumstances did not appear to have materially changed during this review period. Bermuda is seen as an end destination for small, personal arms and ammunition trafficking thought to be primarily linked with the domestic drugs trade, and is neither a producer nor trans-shipment point for large scale illegal arms trafficking.

Given these factors it was determined that the rating of **MEDIUM-LOW** for Illicit Arms Trafficking remains justified in Bermuda, as the proceeds likely to be generated from this crime are not high enough to increase the ML threat rating beyond the level in 2017.

Regarding Commercial Smuggling, there was still no criminal data to rely on for the analysis. The assessment was again based on data from the Customs Department related to action taken on cases of commercial smuggling using powers under the Revenue Act 1898 rather than under criminal laws.

Back to Table of Contents

It was noted that the value of detained imported goods for this offence decreased during the review period, as compared with 2017. The cases in this category also primarily reflected individuals attempting to bring in goods to Bermuda and avoid paying duty, rather than smuggling of goods for resale.

The 2020 analysis went further than the 2017 NRA, moving from estimating the overall value of goods smuggled into the country to focusing on whether this activity could translate into money laundering in real terms. The findings showed that there is no evidence contraband goods are being smuggled into Bermuda for sale on an underground market; there is no underground market for such goods; and cases described in Bermuda as 'commercial smuggling' generally do not match the globally known concept of 'smuggling'. Bermuda also has a specific mechanism for the controlled importation of duty-free items, which makes goods more accessible and affordable through official channels and thus less attractive as contraband. Therefore, the money laundering threat would not be as significant.

Accordingly, it was determined that the rating for this predicate should be lowered to MEDIUM-LOW, given the relatively low likelihood that there would be proceeds from these imports that would lead to money laundering.

IV. Predicate Crimes Ranked as LOW THREAT

Of the 25 categories of predicate offences analysed, it was determined that 14 of them presented a LOW THREAT of money laundering in Bermuda, they included:

- Violent crimes or Crimes Against the Person[18] - it was determined that none posed an ML threat, due to a combination of their generally low numbers and the lack of evidence of associated financial gain for such crimes in Bermuda.

- Acquisitive Crimes (including robbery, theft, handling of stolen goods) - although this broad category of offences accounted for 5582 reports during the review period, law enforcement experience showed that the average value of property gained by criminals who commit such offences remained in the region of $500, making the money laundering potential from such cases negligible.

[18] Kidnapping & illegal restraint; Murder & Grievous Bodily Harm; Sexual Exploitation (including all sexual offences, including those against children); Trafficking in Human Beings.

Back to Table of Contents

- Other offences: Domestic Market Manipulation/Insider Trading, Piracy, Trafficking in Humans/Migrant Smuggling and Transit in Narcotics - all these offences had no reported incidents during the review period. • Environmental crime - only two cases were detected and brought to the courts during the review period and both related to commercial fisheries offences involving low values.

- Transit in Narcotics - was again rated as low threat, but unlike in 2017, during this review period there were no cases where vessels were identified as transiting through a Bermuda port with narcotics on board, for final destination in another jurisdiction. It was acknowledged however, that even if there were undetected instances of this offence occurring, there would be no ML threat to Bermuda derived from it.

Origin of Proceeds of Crime

The 2020 NRA showed that international sources remained a significant factor impacting money laundering in Bermuda. This was reinforced by the predicate offences that were rated as HIGH in the analysis.

I. Domestic Predicate Offences

It was determined that the rating of HIGH for this category remained justified as undetected proceeds from domestic retail drug trafficking would exceed the $10m threshold. Similar to the findings in 2017, Trafficking in Narcotics was shown as being the main driver of money laundering from domestic sources. This predicate also led to the highest number of investigations and prosecutions for ML across all predicates analysed. However, the number of cases which resulted in confiscation and the value of the confiscated proceeds was relatively low, especially as compared to the 2017 ML NRA. Unlike in 2017, there were some ML cases where the proceeds came from other domestic predicates such as fraud and corruption, but their values were relatively low overall when compared to trafficking in narcotics. It was noted that although the majority of ML in this category involved currency conversion and movement of cash across the border, there was evidence that this trend was declining when compared with 2017. Apparently, drug traffickers are relying more on other mechanisms to transfer proceeds, for example, through the use of third-party bank accounts, debit cards and foreign ATMs.

Back to Table of Contents

II. Predicate Offences Committed in a Foreign Jurisdiction

It was determined that a HIGH rating remained appropriate since the cases investigated during the review period, as well as the estimated undetected proceeds from foreign crimes, far exceed the 'high' threshold and actually measure in the hundreds of millions in potential proceeds. As was the case in the 2017 ML NRA, the foreign predicates noted as driving ML in this category continue to be foreign tax crimes, foreign fraud, foreign corruption and insider trading/market manipulation. Local investigations of ML derived from foreign sources were low with no prosecutions during the review period. However, over $18 million was restrained or frozen due to mutual legal assistance requests from foreign counterparts or civil asset recovery actions related to proceeds from foreign crimes being located in Bermuda. Also, the intelligence developed by local authorities, through SAR filings, exchange of information with foreign counterparts and other sources, have reinforced the conclusion that this category represents Bermuda's greatest ML threat, given the potential for large scale ML to occur through the financial system or to be facilitated through the use of complex and sophisticated structures and schemes.

III. Predicate Offences Committed in both Domestic and Foreign Jurisdictions

Compared to 2017, when the only dual-jurisdiction crime identified was drug importation, the 2020 NRA analysis had a wider array of cases within this category, namely drug importation, fraud, cyber-based extortion and insider trading. In the case of drug importation, the analysis showed that a relatively small proportion of the proceeds from retail drug trafficking were sent out of the jurisdiction, as payment for imported drugs. Given the size of the market in Bermuda and the lower cost of wholesale drugs outside of Bermuda, the amount of proceeds generated from drug imports and then laundered and remitted back out of Bermuda is still estimated to be above $1million but under $10 million. However, law enforcement and intelligence authorities have now identified instances of cyber-fraud (phishing and other attacks) and cyber-based extortion (impersonation of CEOs and other executives) occurring in dual jurisdictions, often involving Bermudian victims who are either individuals or legal persons. These cyber cases have now expanded the scale of ML that can occur through dual-jurisdiction criminal activity. Therefore, when the proceeds from the identified cases were considered, along with estimates of undetected criminal proceeds from these types of crimes, it was determined that the potential value of proceeds in this category would reasonably exceed $10 million. On that basis the threat rating for this category of crimes was increased from MEDIUM-HIGH in 2017 to HIGH in 2020.

Back to Table of Contents

IV. Predicate Offences where Country of Origin Not Identified

The rating of LOW in this category remained justified on the basis that detected and undetected proceeds from crimes within it are in the low threshold. The BPS and Customs reported a combined total of 6 cases detected/investigated in this category. Overall, the proceeds associated with the reported cases are extremely low and it was estimated that undetected proceeds from crimes in this category would also be below the $100,000 threshold for this rating. Based on assessing the cases investigated during the review period, Bermuda does not have any material ML threat originating from unidentified criminal sources. This indicates that law enforcement and intelligence authorities in Bermuda are tracing and identifying the sources of criminal proceeds effectively.

Cross-Border Threat Analysis

The 2020 NRA analysis of the cross-border ML threat to Bermuda had additional data for consideration than prior years. This resulted in a greater understanding and more specific breakdown of the level of ML threat posed by individual countries selected on the basis of a) having significant economic touchpoints with Bermuda, and b) frequency of international cooperation in criminal matters and financial intelligence with Bermuda authorities.

Using these criteria, a group of twelve countries was selected for analysis, expanded from eight countries and the Caribbean region in the 2017 NRA, which had been collectively rated as Medium for ML threats. The economic data concerning financial inflows and outflows between Bermuda and each of the selected countries helped develop a picture of the legitimate commercial relationships between them. Analysis was done to better understand the movements of funds associated with trade in goods and services, portfolio investments and foreign direct investments (FDI), as well as the cross-border flow of funds through formal systems, mainly by wire transfers.

The data confirmed that there was significant movement of funds in the FDI, portfolio investment and trade relationships between Bermuda and the United States, the United Kingdom and Canada; while Hong Kong accounts for substantial incoming and outgoing funds mainly due to FDI and portfolio investment. A summary of findings and ratings by country is shown below.

Back to Table of Contents

Countries Rated as HIGH OR MEDIUM-HIGH FOR ML THREAT

(a) United States of America:

The USA ML threat rating of HIGH is largely based on the substantial amount of law enforcement and financial intelligence cooperation, as well as the number and nature of ML related mutual legal assistance and other criminal cases in which the USA is involved. The USA also features in most of the foreign predicate offences determined to be high threat for Bermuda, such as Insider Trading/Market Manipulation, fraud and tax crimes. The USA is the primary trading partner for Bermuda, as well as the primary financial gateway for Bermuda's business, due to the predominance of USD transactions; large scale of inflows and outflows of funds; and the associated correspondent banking and other legitimate commercial ties between both countries. It was determined that illicit proceeds flowed both ways between Bermuda and the USA, with the incoming flow being much higher than the outgoing. Bermuda's threat to the US, primarily through outgoing proceeds from drug trafficking, was rated as being Low due to the relatively low figures involved, and its negligible impact on the US financial system.

(b) India:

It was determined that the rating for India, which was added to the selected countries for analysis, should be MEDIUM-HIGH based on a variety of criminal and civil ML related matters which occurred during the review period. There were various mutual legal assistance (MLA) requests received from Indian authorities (incoming), as well as MLA requests sent from Bermuda to India (outgoing) in relation to proceeds of crime matters, such as to support a USD $10M civil asset recovery case featuring suspected criminal proceeds from India. In addition, SAR filings and other intelligence sources have identified attempts to send questionable MSB transfers to India, as well as multiple queries to the FIA from the Indian FIU, in relation to tax evasion and fraud, both of which are and have been higher threat predicates for Bermuda since 2017. The analysis showed a two-way ML threat between both countries based on the cases examined, with the outgoing threat being more substantial.

Back to Table of Contents

Countries Rated as MEDIUM FOR ML THREAT

(a) United Kingdom:

Although the UK is a significant financial centre with close ties to various Bermuda business sectors, there are a number of factors and features that justify a MEDIUM rating, especially when compared to the threat from the USA. However, it was noted that given the size of the UK's financial centre, there is always the possibility that the threat rating can increase to medium-high or higher if conditions shift. For the period under review, while the business profile between Bermuda and the UK is similar to that between Bermuda and the USA, the scale of business with the UK was significantly smaller. Even though there are a large number of clients from the UK, overall the business has a generally lower dollar value, compared to the USA. The analysis determined that illicit funds flow between the countries mainly as incoming proceeds to Bermuda. This conclusion took into account reports from law enforcement of a minimal amount of proceeds going to the UK from Bermuda during the review period, related to one fraud case.

(b) Canada:

The MEDIUM threat rating for Canada reflects the relatively lower size and scale of business with Bermuda, especially when compared with the US and UK. Financial intelligence did not pose Canada as a leading source of ML threats. The numbers and types of cases, and proceeds detained, frozen or restrained were also considered, along with international cooperation requests. The ML threat was assessed to be two-way. However, the majority of the threat was incoming rather than outgoing, with intelligence pointing to securities fraud and drug trafficking as the predicates. Outgoing criminal proceeds appeared to relate to either foreign tax evasion relating to expatriates' locally generated income; or local drug trafficking proceeds.

Countries Rated as MEDIUM-LOW OR LOW FOR ML THREAT

All of the remaining countries selected for this analysis were rated with MEDIUM-LOW or LOW. This includes Germany, France, Switzerland, the Netherlands, Luxembourg, Japan, China, and Hong Kong. Notably, while Hong Kong and China received lower ML threat ratings, it was acknowledged that their geo-political relationship should be monitored closely for any potential impacts on Bermuda's economic ties and substantial investment flows with Hong Kong.

Back to Table of Contents

Summary - Sector-Specific ML Threat Analysis

Available statistical data on money laundering cases investigated and prosecuted assisted in identifying which sectors were at HIGHER RISK for ML threats. Intelligence from FIA disseminations, based on suspicious activity reports filed with the FIA, were also useful in this analysis. Also, while respecting OECD[19] confidentiality rules, the Ministry of Finance was able to provide data about sectors in Bermuda affected by tax information requests from other countries. Other factors considered included the size of each sector within Bermuda's economy, and the estimate of undetected money laundering activities in each sector.

From this analysis, it was determined that the money laundering threat was HIGH in the Banking & Credit Union, Securities, Trust Business, Corporate Service Providers and Legal sectors. This was an increased threat rating for the Trust and Legal sectors in particular, from medium-high in 2017. The Long-Term (Life) segment of the Insurance sector, which is subject to AML/ATF supervision, retained the threat rating of MEDIUM/HIGH, while the Money Service Business sector was lowered from MEDIUM-HIGH TO MEDIUM.

Further details of the sectoral ML threat analysis with sector-specific ratings are provided later in this report.

Conclusion

In light of all of the factors outlined above, it was determined that Bermuda's overall ML Threat rating is HIGH. This is a shift from the Medium-high rating in 2017. This rating reflects changes in patterns of the relatively small group of predicate crimes driving ML threats to Bermuda since that time. It is also based on deeper analysis and understanding of Bermuda's potential ML risks using a wider range of data and information available for the 2020 NRA.

The fact remains that Bermuda's most significant money laundering threats are predominantly based on criminal activity carried out overseas. As Bermuda's economy is largely supported by international financial business, it has a greater exposure to foreign-sourced money laundering threats in the sectors that comprise and support this business. The type and scale of potential money laundering from relevant foreign crimes, such as fraud, market manipulation and corruption, pose a high ML threat to Bermuda's financial system, given the volume of financial services business conducted internationally.

Domestically, the proceeds from retail drug trafficking still represent the highest threat of locally-sourced ML within Bermuda; all other domestic predicates were rated as Low. Domestic fraud, as well as other two-way offences such as importation of drugs and cyber-based extortion, also potentially contribute to ML threats in Bermuda. Notably however, considering the scale of potential ML from these sources, domestic predicates overall still pose a significantly lower threat to Bermuda than ML threats originating from foreign sources.

[19] The Organisation for Economic Co-operation and Development's (OECD) Global Forum on Transparency and Exchange of Information for tax Purposes is focused on implementing international standards to end bank secrecy and tax evasion through global tax co-operation. The Global Forum has strong confidentiality rules for countries to preserve the integrity of the tax information requested and shared bi-laterally or multi-laterally.

Back to Table of Contents

Chapter 6: The Deposit-Taking Sector

Summary Findings: The assessment of Bermuda's deposit-taking sector, which included an enhanced, granular analysis of 22 sectoral products, resulted in an inherent vulnerability rating of MEDIUM. The National Threat Assessment determined that the sector had a ML threat rating of HIGH. The resulting inherent ML risk rating for the sector was MEDIUM-HIGH.

AML/ATF Supervisory Authority – Bermuda Monetary Authority

Introduction

Bermuda's deposit-taking sector consists of five entities: four banks and one credit union. The sector is significant relative to the size of the overall economy: as at the end of 2019 the sector had approximately $24 billion of assets and total income of $894 million, the latter being equivalent to 7.2% of GDP.

Banks in Bermuda offer a sophisticated range of financial products and services to a wide range of clients. These products and services cover Retail and Business Banking (for local residents); Corporate and Transaction Banking (mostly for international companies domiciled in Bermuda); and Wealth Management and Private Banking (for both domestic and foreign high net worth individuals).

As a result, in addition to servicing the banking needs of Bermuda's resident population, Bermudian banks also service Bermuda's international business sector with other regulated sectors, and tailor Corporate Banking services to support the Bermuda economy, with a particular focus on the captive insurance market.

The one credit union has total assets of less than 0.001% of the total financial assets in Bermuda. The credit union provides services to residents only, with a further requirement that they are members of a local union. Due to the size of the credit union and its minor impact to ML vulnerabilities compared to the banks, the analysis below focused solely on bank-based products.

Assessment of Sectoral ML Threats

The ML threat rating for Bermuda's banking sector was HIGH. This rating is driven by two primary factors: the significant size of the sector when compared to the size of the overall economy in Bermuda; and the sector's exposure to international businesses and global cross-border transfer of funds.

The sector featured in 56 money laundering investigations and in 4 prosecutions, which resulted in 3 convictions. Whilst the banking sector's enhanced monitoring and detection capabilities continue bearing fruit, the investigation numbers indicate a shift in typologies within reported ML activity. In the 2017 assessment, the only SARs received from this sector related to currency conversions associated with laundering of drug trafficking proceeds. During the 2020 NRA review period, the FIA reported receiving SAR and STRs in respect of an additional range of suspected criminal activity, e.g. outgoing and incoming wire transfers, suspected CEO impersonation fraud in one report, and the use of debit cards involving Bermudians linked to persons overseas. It should also be noted that since 2017 there has been a decline in currency conversions from Bermuda dollars to USD in banks. This has been associated with suspected changes in the methods used for transferring

Back to Table of Contents

drug trafficking proceeds out of the country. It appears that money launderers are transporting multiple third party debit cards out of the jurisdiction instead of cash. They then use overseas ATMs to extract USD from these third party accounts in Bermuda, as opposed to physically transporting USD cash out of the country.

Overall it remains that the threat of Bermuda's banking sector being targeted for ML purposes from foreign sourced criminal proceeds is higher than from domestic criminal conduct, e.g. international tax crimes, international market manipulation and insider trading and international fraud. The more complex the scheme and the more advanced the stage of ML (i.e. placement, layering or integration), the more challenging detection of these activities becomes. Given Bermuda's substantial international business sector, and the services provided to some segments of that business by the banking sector, their exposure to this potentially greater scale of ML threats remains HIGH.

Analysis of Sector Inherent ML Vulnerabilities

The inherent ML vulnerability rating for the sector was MEDIUM. In the 2017 NRA the product assessment, which is the foundation of the inherent vulnerability rating, was based purely on the client segments of the sector - Retail, Commercial and Wealth Management/Private Banking - as per the risk based approach guidance issued by the FATF for the banking sector. The 2020 NRA approach assessed the products and the underlying client segments in more granular detail, and used the product analysis to support the vulnerability assessment of the three client segments.

Overall, 22 products were identified and assessed; a brief overview of each client segment and the higher vulnerability products used by each is given below. The product segment of Payment Services and Electronic transfers is offered to all segments, and was therefore assessed separately. The product assessment showed that cash products (foreign cash exchanges & bank drafts), deposit products (demand deposits & safety deposit boxes) and wire transfers (domestic & foreign wires) represent the highest inherent vulnerability.

Retail and Business Banking has MEDIUM-HIGH inherent vulnerability. The client profile for Retail and Business banking is predominantly Bermuda residents. As typical in most jurisdictions, the vulnerability associated with retail deposit accounts is their potential to facilitate quick and multiple transfers in the layering of proceeds of crime. This is due to the number of clients involved, the wide range of products offered and high transaction volumes.

In Bermuda's retail banking sector, products with the highest vulnerability to ML activity remain the use of cash in demand deposits, safe deposit boxes, foreign exchange cash products and domestic and foreign wire transfers.

Cash transactions are typically focused within the domestic market, however, the conversion of Bermuda currency to foreign exchange in cash remains an inherent vulnerability. Key features of deposit products include high frequency, high value domestic transactions and the ability to conduct non-face-to-face transactions. However, non-face-to-face transaction record keeping is very detailed, reducing ML risk. Similarly, while ownership details

Back to Table of Contents

of safe deposit boxes are well-recorded, the inherent risk of this product continues to be the unknown value of assets stored in them[20].

Commercial Banking has HIGH inherent vulnerability, driven by the high number of international companies and high volume of international transactions. Commercial products include commercial banking (deposits), commercial loans and mortgages. From a global perspective, such products may be abused for ML purposes. Credit products characteristically have a high inherent vulnerability, due to the total value, higher risk client profile and frequency of international transactions. Bermuda's client base profile for commercial banking consists of corporate domestic and international business clientele. The high volumes of cross-border transactions conducted for international business clients in particular presents inherent vulnerability.

The complex transactions and multiple parties involved in trade finance also presents ML vulnerability globally. In Bermuda, use of trade finance products in this segment, primarily trade letters of credit and standby letters of credit used by the insurance sector, is minimal in terms of value and volume of transactions. **Wealth Management and Private Banking has MEDIUM-HIGH inherent vulnerability**. Wealth management products include: mutual funds (which accounts for 67% of the sector's total wealth management products), discretionary asset management and retail brokerage. Wealth management products are typically characterised as low volume transactions with high values. Given the nature of such products, which generally involve complex services aligned with client confidentiality, they are regarded as inherently vulnerable to ML risk, e.g. tax evasion, political corruption. In Bermuda the products span both domestic and overseas high net worth individuals. Within the sector only two out of the five institutions offer private banking services. Wealth management products have the ability to support non-face-to-face transactions, however the potential for anonymity is extremely limited due to rigorous KYC practices and long-established client relationships, and record keeping is very detailed.

Payment Services and Transfer of Funds have a HIGH INHERENT vulnerability. Wire transfers include domestic and foreign transfers, with the latter regarded as carrying a higher inherent ML vulnerability. Wires are higher in inherent vulnerability given the high volume and value of transactions involved, the wide use of this product across all client types (domestic and international) and the international cross-border nature of the transactions.

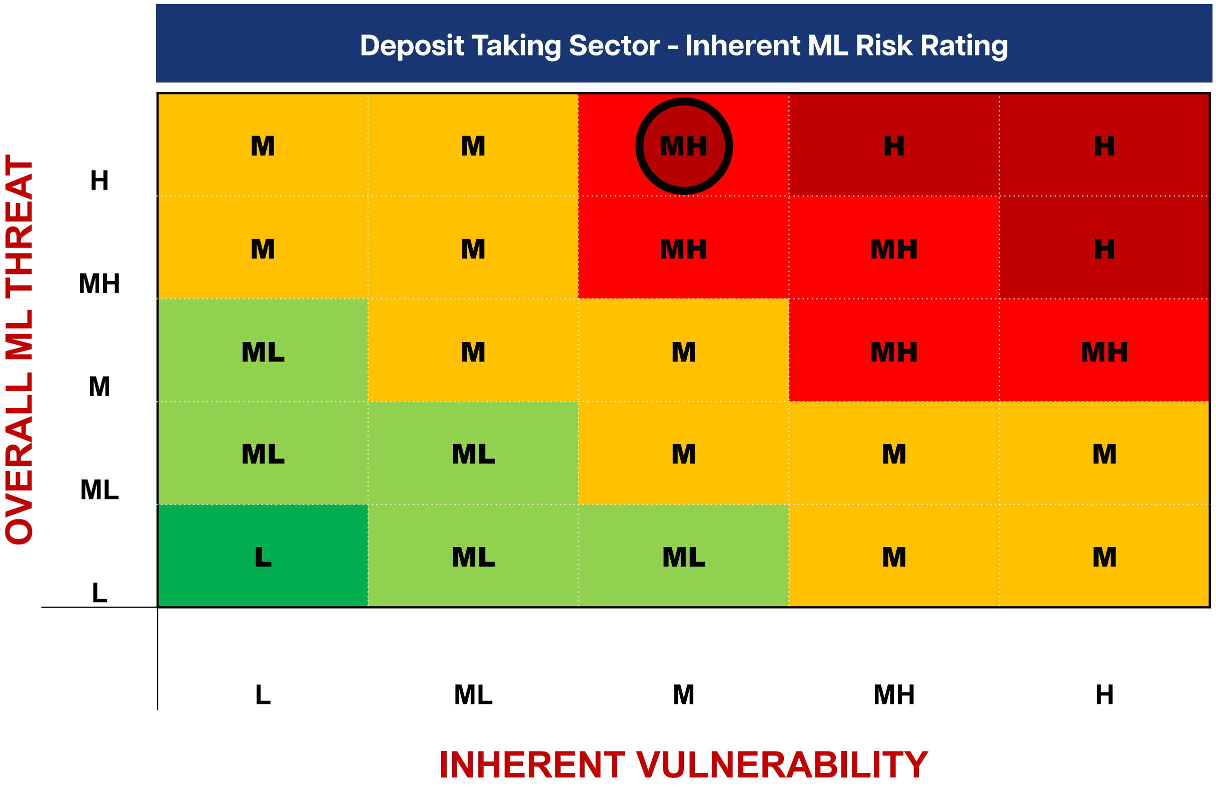
Monitoring differences between the total value and volume of wires being sent to specific overseas jurisdictions can also be a factor for banking institutions to assess potential cross-border risk to Bermuda. Through 2017 to 2019, there were a total of 727,000 incoming wires with a value of $841 billion; and a total of 1.05 million outgoing wires with a value of $835B. The top jurisdictions for outgoing wires by value were USA, United Kingdom, Cayman Islands, Canada and Switzerland, whereas by volume were USA, United Kingdom, Canada, Philippines and Switzerland. The top jurisdictions for incoming wires by value were USA, United Kingdom, Canada, Ireland and Guernsey, whereas by volume were USA, United Kingdom, Ireland, Canada and Switzerland.

[20] FATF Recommendation 12 requires a document of reliable personal identification to open a safe deposit box, but no requirement for the owner to disclose the box's contents.

Back to Table of Contents

Conclusion

The assessment of the deposit-taking sector, which included an enhanced, granular analysis of 22 sectoral products, resulted in an inherent product vulnerability rating of MEDIUM. The National Threat Assessment determined that the sector had a ML threat rating of High. The resulting ML risk rating for the sector was MEDIUM-HIGH, as shown in the heat map below.



Deposit Taking Sector - Inherent ML Risk Rating

OVERALL ML THREAT					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

INHERENT VULNERABILITY

Back to Table of Contents

Chapter 7: The Insurance Sector

Summary Findings: For the purposes of AML/ATF regulation, and ongoing NRA reporting, Bermuda's insurance sector is divided into two groupings:

AML/ATF Regulated Insurance - has a MEDIUM-HIGH inherent ML risk, based on a medium-high ML threat rating and medium inherent vulnerability rating, and driven primarily by the nature of the products offered and the predominantly international client base served.

General business and reinsurance - has a MEDIUM-LOW inherent ML risk rating, based on a low ML threat rating and medium-low inherent vulnerability rating, as the majority of clients are either related to the insurers in this category themselves (e.g. as a parent or affiliate company), or are other regulated insurance entities.

Each sub sector's ML vulnerabilities have been assessed independently to reflect the underlying business conducted within it.

AML/ATF Supervisory Authority – Bermuda Monetary Authority

Introduction

As of 2019 the Bermuda insurance sector's US$980 billion in assets. The insurance sector remains the largest financial sector in Bermuda's economy, with extensive global reach. With 1,201 registered insurance entities, Bermuda is one of the largest reinsurance centres in the world, and the leading captive insurance company domicile. It also remains the leader in insurance-linked securities (ILS) issuing a significant percent of global ILS capacity in 2019, as well as the leading jurisdiction in issuing catastrophe bonds.

The two insurance sub-sectors categorised for the purposes of AML/ATF regulation are detailed as follows:

- **AML/ATF Regulated Insurance** - long-term direct (life) insurance companies (e.g. direct life insurer and long-term annuities), insurance managers, insurance brokers and the new insurance marketplace providers and brokers that deal specifically with Long-Term Insurers writing direct business. This group is AML/TF regulated, under POCA and related Acts and Regulations.
- **General business and reinsurance** - captive insurers (Limited Purpose Insurers) and commercial insurers writing direct general business, reinsurers assuming general and/or long-term insurance, and Special Purpose Insurers (SPIs). This group is not AML/ATF regulated, but required by legislation to have policies and procedures in place for reporting suspicious activities, and is included in Bermuda's risk assessments.

This division of Bermuda's insurance sector aligns with global standards and guidance related to AML/ATF regulation of the industry, based on the FATF's Core Principles and documented by the IAIS.

During the review period, the insurance marketplace providers segment was brought within scope of AML/TF regulation. An insurance marketplace provider is a category of insurance intermediary, providing solutions through the growing use of technology. The concept of an "insurance marketplace" is a platform, of any type, established for the purpose of buying, selling or trading insurance contracts.

Back to Table of Contents

Analysis of ML Threats

The ML threat rating for the AML/ATF Regulated Insurance sub-sector remained at MEDIUM-HIGH, driven by the long-term direct segment. There were four ML investigations which were associated with this segment during the review period; $10 million in suspected proceeds frozen in a life insurance policy in pending civil recovery proceedings; and 41 intelligence disseminations from the FIA, derived largely from suspicious transaction reports filed by the sub-sector. Foreign predicate offences were the main subjects of the intelligence reports associated with this sub-sector, namely, corruption/bribery, fraud and tax offences, and in total the associated transactions or policies had a high dollar value measured in hundreds of millions. Therefore, the scale of proceeds that can potentially be laundered through this sector is significant, particularly because the ML threat to this sector is mainly connected with the global distribution of its insurance business. The other segments of this sub-sector, i.e. insurance managers, insurance brokers and insurance marketplace providers, have a different profile and are less exposed to ML threats. In the long-term direct segment, 98% of the business is foreign (in line with Bermuda's national ML threats primarily being sourced from overseas), while in the insurance management segment the entirety of the client base is domestic.

Bermuda's general business and reinsurance sub-sector was assessed to have a low ML threat rating, also unchanged from 2017. There remained no evidence that the institutions or products in this sub-sector were or could be used successfully in ML activity.

Analysis of Sectoral Inherent Vulnerabilities

A. AML/ATF Regulated Insurance

The ML inherent vulnerability rating for this sub-sector was MEDIUM. The scope of analysis for the sub-sector was updated in 2020 to assess product risk across segments within it. In 2017, due to data limitations, the analysis was structured and assessed solely based on the client base. For the 2020 NRA, a more detailed product structure was adopted, allowing for a more granular assessment.

The analysis of inherent vulnerability factors specific to products were aligned with four key segments within the sub-sector:

i. Long-term direct insurance

The ML inherent vulnerability rating for the long-term direct insurance sector was MEDIUM-HIGH. This is driven primarily by the nature of the products offered and the predominantly international client base served. For long term direct insurers the client profile in terms of Gross Premiums Written (GPW) is predominantly from South East Asia (64%); and from Southern Africa (35%). These jurisdictions are also prominent for the long term direct insurance sub-sector in terms of the number of beneficiaries, claims paid, number of policies written and the number of PEPs.

Back to Table of Contents

ii. Insurance managers

The average ML inherent vulnerability rating for the insurance managers was MEDIUM. The client base profile of insurance managers and direct LT insurers differs significantly, impacting their respective inherent ML vulnerability. Insurance managers only service regulated Bermuda insurance companies and as a result have a lower inherent vulnerability. Direct LT insurers, who service an international customer base, have a higher inherent ML vulnerability.

iii. Insurance marketplace providers

The insurance marketplace provider ML inherent vulnerability rating was MEDIUM-LOW. There were no insurance marketplace providers licensed during the review period, as it was a newly introduced segment. However, each area outlined below can be considered as a risk factor related to this segment from which ML risks may emanate:

> Client profile/participants - insurance marketplace providers will act as intermediaries, bringing together buyers and sellers in insurance transactions via specific trading platforms. This may also include any parties in between that play a role in the whole insurance life cycle. Importantly, the intended participants are already regulated for AML/ATF requirements or are at minimum required to report suspicious activity, e.g. LT insurers and reinsurers, insurance managers, brokers and agents, capital providers.
>
> Type of business - insurance marketplace providers will report the type of business placed in their platforms, and obtain confirmation from the parties involved in transactions that they have complied with required AML/ATF responsibilities.

iv. Brokers (servicing long term direct insurance)

There were no brokers servicing long term direct insurers during the assessment period as a result there were no products or services to analyse.

B. General Business and Reinsurance

The general business and reinsurance sector's average ML inherent vulnerability rating was MEDIUM-LOW. Despite the general nature of the business not creating AML/ATF vulnerabilities, this rating reflects the significant size and importance of the insurance sector in Bermuda, and its diverse international customer base. There are two segments within this sub sector:

Back to Table of Contents

i. General business/Reinsurance

The general business and reinsurance segment has a ML inherent vulnerability rating of MEDIUM-LOW. This rating is driven by the segment's diverse international and domestic customer base and its large size.

ii. Long-term reinsurance

This segment also has a ML inherent vulnerability rating of MEDIUM-LOW, based on its average transaction size and international clients who are related to regulated insurance entities.

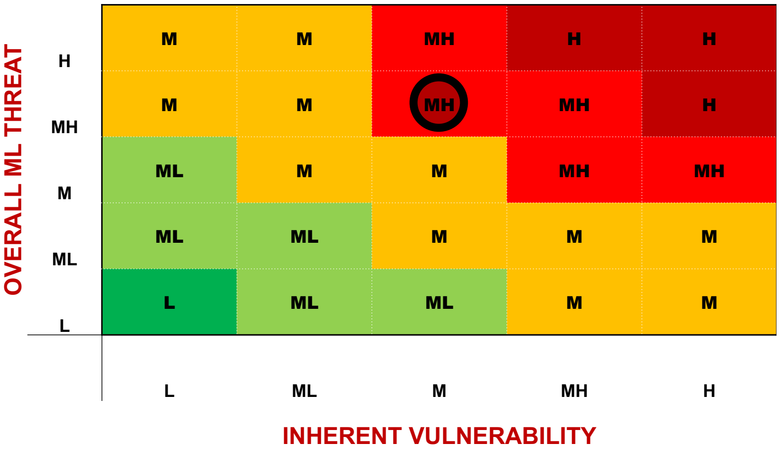
In terms of geographic vulnerabilities, the vast majority of gross premiums were generated from policyholders who live in jurisdictions that are regarded as presenting a lower AML/ATF threat i.e. (Bermuda (44%), followed by North America (37%), Europe (11%), Australia and New Zealand (2%).

Conclusion

The ML risk ratings for Bermuda's insurance sector, assessed for AML/TF purposes in two distinct sub-sector groupings based on the underlying business each group conducts, is shown below and summarised in respective sub-sector heat maps:

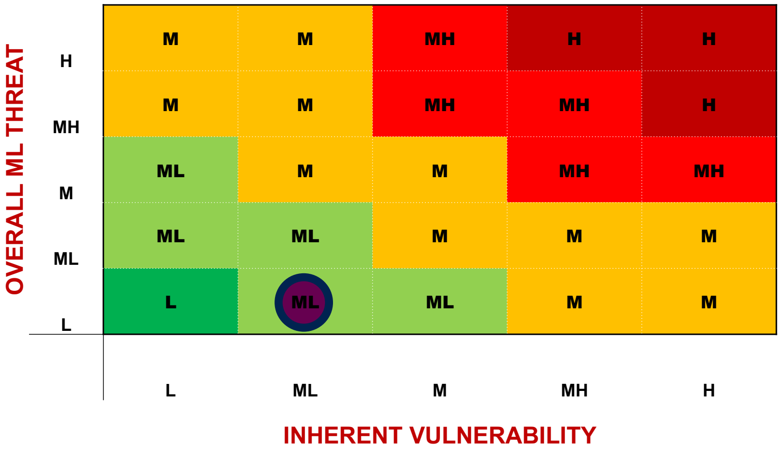
- AML/ATF Regulated Insurance sector has a MEDIUM-HIGH ML risk, based on a MEDIUM-HIGH ML threat rating and MEDIUM inherent vulnerability rating
- General business and reinsurance has a MEDIUM-LOW ML risk rating, based on a LOW ML threat rating and MEDIUM-LOW inherent vulnerability rating.

AML/ATF Regulated Insurance Sector – Inherent ML Risk Rating



	L	ML	M	MH	H
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M

General Business & Reinsurance Sector – Inherent ML Risk Rating



	L	ML	M	MH	H
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M

Back to Table of Contents

Chapter 8: The Securities Sector

Summary Findings: The overall ML risk rating for the Securities sector is HIGH, reflecting the MEDIUM-HIGH rating for inherent vulnerabilities and the high rating for ML threats. This rating takes into account features that characterise the securities industry, including the variation in products, global reach, and scale and volume of international transactions.

AML/ATF Supervisory Authority – Bermuda Monetary Authority

Introduction

Bermuda's Securities sector is well developed and offers a sophisticated range of products. The Securities sector in Bermuda is primarily regulated by the following Acts: The Investment Funds Act 2006 (IFA), the Investment Business Act 2003 (IBA), the Fund Administrator Provider Business Act 2019 and the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (SEA). The sector consists of:

- Investment Businesses, which may act as Investment Managers, Broker-Dealers, or both, under the Investment Business Act 2003;
- Non-Licensed Persons, which are financial institutions exempted from the Investment Business Act 2003 (Section 13) by the Investment Business (Exemptions) Order 2004 ("IBA exempt");
- Fund Administrators, under the Fund Administrator provider Business Act 2019;
- Investment Funds, under the Investment Funds Act 2006.

The sector has 52 licensed investment businesses and 31 licensed fund administrators. There were 638 registered investment funds in the reporting period. In December 2019, the investment funds had a total Net Asset Value of approximately $176 billion. In December 2019, there were 76 registered NLPs.

Assessment of Sectoral ML Threats

The Securities sector ML threat rating was high. Globally in the securities sector, the "gatekeeper" function of investment managers and fund administrators with respect to investors - along with the international reach, product complexity, volume of transactions and client base profile - present inherent exposure to ML threats. In that context, Bermuda's securities sector faces similar exposures and it was determined that the ML threat to this sector remains high, particularly the threat of ML sourced from overseas. The fact that the sector is a significant contributor to Bermuda's economy and a prime component in Bermuda's international business sector also underpins this rating.

There were 3 local investigations involving this sector during the review period, and approximately $4 million, suspected to be proceeds from foreign real estate and bank frauds, was frozen under the civil asset recovery regime. Since two civil asset recovery cases were still pending during the NRA, no funds were confiscated during the period. However, approximately $3.5 million of funds related to these cases remain frozen.

The FIA reported that the intelligence received involving this sector originated mainly from 54 STRs and 33 SARs, together with some incoming overseas requests. The STRs involved transactions totaling

Back to Table of Contents

approximately $627 million. Although just 1 of the STRs was associated with a declined transaction of $500 million, the remaining $127 million value in transactions was still much higher than the total value of transactions reported in the previous review period, which amounted to $84 million. The main predicate offence identified was fraud, with other offences being corruption, insider trading and tax offences. The findings for tax offences is corroborated from incoming overseas requests on criminal tax information received by Bermuda, in which different segments[21] within the securities sector featured in the requests received in each of the 3 years of the 2017 – 2019 review period.

Analysis of Sector Inherent ML Vulnerabilities

Since the last ML NRA in 2017, amendments to the Investment Funds Act 2016 changed the classifications of investment funds, impacting how the assessment of the products in the securities sector was conducted in this NRA.

Also, in December 2017, Bermuda implemented legislation for the EU's economic substance requirements applicable to international businesses operating in or from some third countries. This was as part of Bermuda's ongoing commitment to assist the EU in combating harmful tax practices.

From January 2019, the amended legislation required exempted (Class A/B) and excluded investment funds to be fully regulated for prudential and AML purposes. These fund types are now referred to as "Professional Class A Fund", "Professional Class B Fund" and "Private Fund" respectively.

The extent of AML/ATF regulatory controls, supervision, and monitoring varies depending on the specific licence obtained, the type of interaction with the client and in accordance with the BMA's risk based approach to AML/ATF supervision. As such the assessment of the product-based vulnerability factors was split based on the three key sub-sectors within Bermuda's Securities sector listed below, while taking into account their respective product or service lines available to the client:

i. **Investment Business: In Bermuda, the Investment Businesses sub-sector consists of investment managers and investment broker-dealers.** Investment broker-dealers are considered to have a medium-high inherent vulnerability, a result of their fluid buying and selling, rapid series of one-off transactions, reliance on financial institutions and heavy client interaction, as they typically deal with a low volume of high value customers. Client relationships typically involve frequent face-to-face contact, and an ongoing relationship management which involves a deep understanding of the client's financial circumstances.

   The MEDIUM HIGH inherent vulnerability rating is also driven by the sub-sector's international nature and high volume

[21] In 2017, a Mutual Fund was affected/involved in at least 1 of 5 criminal tax information requests; in 2018, investment holding/trading firm(s) were involved in one or more of the 65 criminal tax information requests received; and in 2019, Mutual Fund(s) and investment holding/trading firm(s) were involved in one or more of the 23 criminal tax information requests received by Bermuda.

Back to Table of Contents

of cross-border transactions, technical complexity and client base profile (high net worth individuals (HNWI), including PEPs). In Bermuda, the majority of assets remain concentrated in discretionary investment management, where investment decisions are made on the client's behalf within the parameters of a set investment mandate agreed in advance, and periodically reviewed with the client. This limits a client's ability to engage in market manipulation, insider trading or securities fraud. The vulnerability of non-discretionary investment management is perceived to be greater due to the more client-driven nature of the relationship; the investment manager primarily advises clients on investment strategies, but the client makes the investment decisions and the investment manager executes the resulting transactions.

ii. **<u>Fund Administrators and Investment Funds:</u> The investment funds sub-sector is assessed to have MEDIUM-HIGH inherent vulnerability due to its international nature, high volume of cross-border transactions, technical complexity and client profile base.** In 2019, the total number of administered funds in Bermuda was 2,169 of which 512 of the 638 Bermuda-registered investment funds were locally-incorporated funds. Of the Bermuda-registered investment funds, 80% were serviced by a Bermuda Fund Administrator.

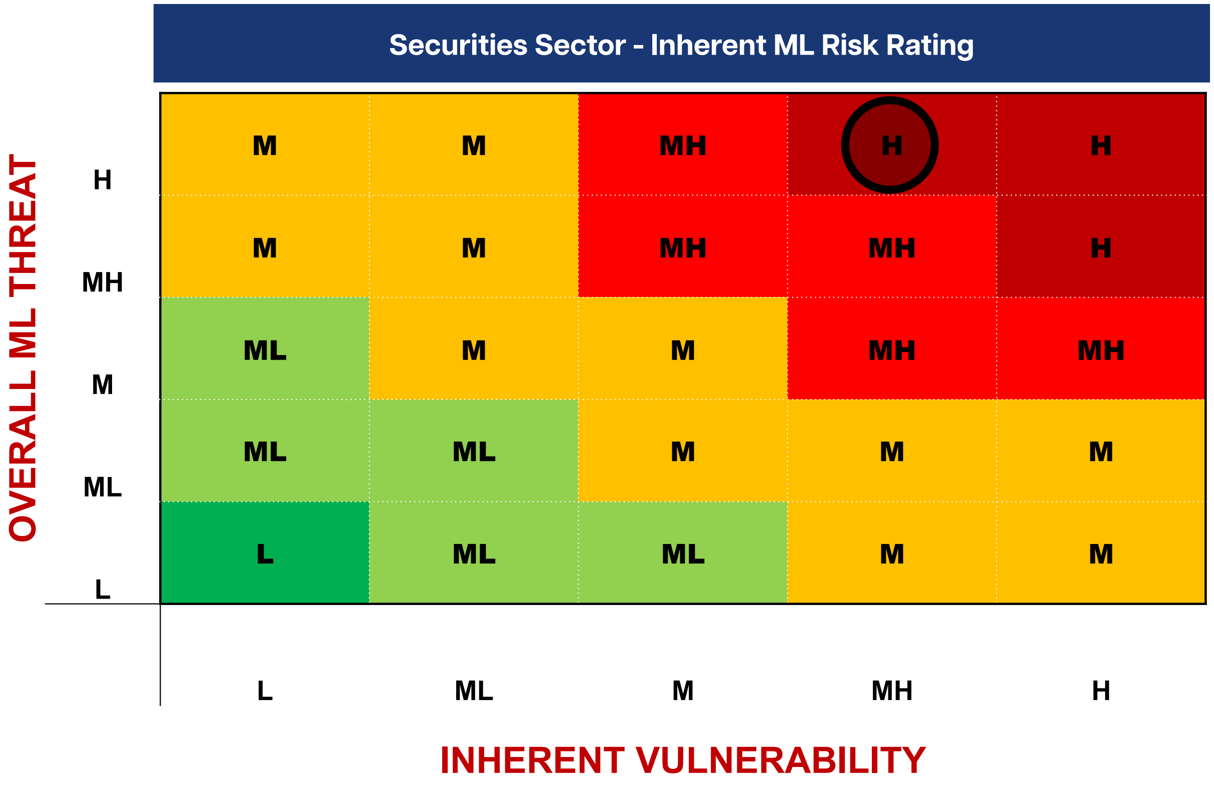
The client base profile of the fund administrators and investment funds is assessed as MEDIUM vulnerability. It should be clarified that the clients of fund administrators are the funds themselves, which are regulated separately from their fund administrators for AML. For investment funds, the clients are the investors in the funds. The proportion of the fund administrators' client base of PEPs and HNWI is more modest than for the client base of investment funds. Clients of investment funds (i.e. the investors) tend to be HNWI, institutional or sophisticated investors, with the exception of Authorised Standard Funds which may include a more significant retail element among their investors. Consequently, Authorised Standard Funds are subject to more comprehensive regulation and supervision. Similar to the Investment Business sub-sector, an investor must meet the required customer due diligence prerequisites prior to submitting a subscription. These are often detailed in the investment fund's prospectus, and include requirements such as remitting subscriptions from an account with a regulated bank and providing evidence of source of wealth or source of funds.

iii. **<u>Non-Licensed Persons (NLP):</u> NLPs were determined to have a MEDIUM-HIGH inherent vulnerability.** The rating was driven primarily by the client profile (involving HNWI, PEPs and sophisticated investors) and associated asset size of investors associated with NLPs. For example, registered NLPs often engage with a substantial proportion of international PEPs. In comparison to the investment business sub-sector, the NLP sub-sector has fewer clients, most of whom are predominantly discretionary managed investments clients.

Back to Table of Contents

Conclusion

The ML risk rating for the Securities sector consists of the MEDIUM-HIGH rating for inherent vulnerabilities and the High rating for ML threats, resulting in an inherent rating of HIGH. This is shown in the heat map below.



Securities Sector - Inherent ML Risk Rating

OVERALL ML THREAT					
H	M	M	MH	[✓ H]	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H
	INHERENT VULNERABILITY				

Back to Table of Contents

Chapter 9: Money Service Businesses (MSBs)

Summary of Findings: The inherent ML risk rating of medium for the MSB sector comprises a medium rating for inherent vulnerability, which included an enhanced analysis of 7 sectoral products, and a medium rating for ML threat. This is primarily due to the small size of the MSB sector in Bermuda; the small volumes and values of money transacted through the three MSBs in it; and the sector's modest impact on the financial industry as a whole.

AML/ATF Supervisory Authority – Bermuda Monetary Authority

Introduction

The Money Service Business Act 2016 ("the Act"), which came into force on the 31st January 2017, regulates MSBs in Bermuda, and sets out a licensing regime for the undertaking of Money Service Business. Under Section 2(2) of "the Act" "Money Service Business" is defined very broadly, and can encompass a wide range of services. These range from money transmission services, cheque cashing, payment services, and operating bureaus de change. There were 3 MSB entities licensed at the end of the review period, which spans January 2017 to December 2019, although not all entities were conducting money transmission services throughout the entire period.

Any business operating as an agent of Money Service Business in Bermuda must be licensed in their own right, which further enhances the controls over the potential risks posed by this sector and greatly facilitates supervision. During the review period, the MSB sector transacted approximately $95 million of outgoing money transmissions.

The core market of MSBs in Bermuda is Bermuda residents, which includes guest workers, and occasionally tourists sending or receiving money. The primary service in the sector is money transmissions, i.e. outward remittances. The primary jurisdictions receiving outward money transfers from MSBs were Jamaica, Philippines, USA, Portugal and Dominican Republic.

Assessment of Sectoral ML Threats

The ML threat rating of MEDIUM for the MSB sector was lower than in 2017. As was noted in 2017, the sector continues to monitor for suspicious activity and submits quality SARS, declining suspicious transactions and reporting to the FIA whenever there are suspicions (whether or not the business was declined). Based on intelligence gleaned from SARs and other sources, the nature and volume of suspected criminal proceeds during the review period was assessed to be less than $1 million. Therefore, although the sector submits a high volume of SARs, the medium rating is justified, based on a combination of factors**:**

- The sector remains small in the context of Bermuda's economy, with a relatively limited overall volume of transactions; this directly affects the scale of criminal proceeds that can be moved through this sector.
- Licensed operators within the sector have also set limits on the value of funds that can be remitted in a single transaction, further limiting the amount of proceeds that can be moved.

Back to Table of Contents

- Given the size of the sector and the few operators in business, the clientele is well known to the operators, thus further limiting the opportunity for smurfing to circumvent the transactional limit.
- The client base of MSBs are mainly foreign workers in the hospitality and other service sectors sending funds home to their families. This type of client base therefore has a certain profile in terms of the volume of funds being remitted and the frequency. The majority of transactions conducted during the review period were below $1,000 in value, significantly reducing the likelihood of ML taking place in any material way.

Analysis of Sector Inherent ML Vulnerabilities

The inherent ML vulnerability rating for MSB products was MEDIUM. As noted above, there were 3 MSB entities licensed at the end of the review period, although not all the entities were licensed or conducting money transmission services throughout this entire period. Seven products were assessed: money transmission services, cheque cashing, electronic payments, merchant payments, foreign currency exchange services, credit card payments (AMEX) and internet bill payments. Of the assessed products offered by the MSBs, the products with the higher inherent risk include: money transmission services, cheque cashing and foreign exchange services.

Globally, MSBs typically have high inherent vulnerability to ML. However, in Bermuda the MSB business model is materially different to the global model in two respects**:** there are no unlicensed or unsupervised agents in operation; and customers tend to be repeat, and therefore well-known to the MSBs due to the small size of the country and the small size of the sector. The general characteristics of the MSBs' services in Bermuda are cash-based, low value, and the ability to conduct cross-border transactions far more conveniently than through the banks.

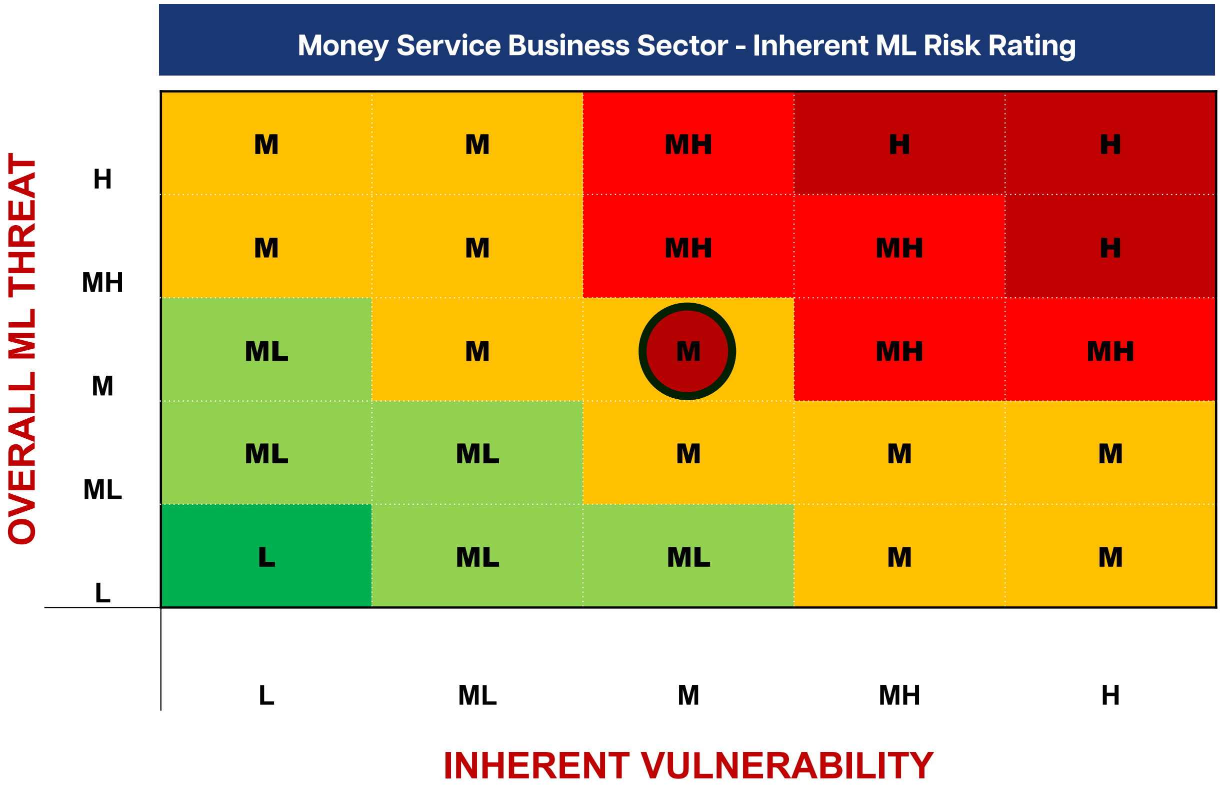
The client base profile presents a high ML vulnerability to MSBs for their money transfer services, cheque cashing and foreign currency exchange services. Bermuda's core MSB market consists of local residents and tourists that arrive via cruise ships or international flights. The local resident clients include foreign guest workers sending money to their countries of origin. Resident MSB clients may be underserved by the banks or choose not to use the banks, potentially for cost reasons. Case studies conducted by the FIA include many involving MSBs and the FIA has concluded that the staff of MSBs in Bermuda turn away clients that they deem as suspicious, indicating a high degree of awareness, training and effectiveness by the MSBs towards ML or TF threats.

The level of cash activity and frequency of international transactions were both assessed as HIGH. During the review period of 2017 to 2019 there were 10,704 inward transactions totaling $3.8 million and 269,320 outward transactions totaling $95 million, which constituted the largest service offered by the MSBs. Although the MSB sector is responsible for the highest numbers of SARs filed with the FIA annually (compared to other sectors), the average dollar value involved is comparatively very low.

Back to Table of Contents

Conclusion

As shown in the heat map below, the ML risk rating of medium for the MSB sector comprises a medium rating for inherent vulnerability and a medium rating for ML threat.



Money Service Business Sector - Inherent ML Risk Rating

OVERALL ML THREAT \ INHERENT VULNERABILITY	L	ML	M	MH	H
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M

Back to Table of Contents

Chapter 10: The Lending Sector and Financial Leasing

Summary of Findings: The Lending sector has a low ML threat rating, due to the small size and nature of the sector. When combined with the inherent vulnerability rating of medium-low, the Lending sector is assessed as having a medium-low inherent ML risk.

There are currently no regulated entities performing financial leasing, therefore this chapter focuses on the Lending sector.

AML/ATF Supervisory Authority – Bermuda Monetary Authority

Introduction

Lending and Financial Leasing were brought into scope for AML/ATF regulation under the Proceeds of Crime Act 1997 in September 2018 and accordingly, the lending sector has since been supervised by the Bermuda Monetary Authority. Under Section 42A and further referenced under Schedule 3, any entity carrying on specified financial activity must be subject to AML/ATF regulatory requirements and supervision, through a system of registration with the Authority. Schedule 3(1)(b) was amended to expand the definition of specified financial activity to include “lending, including consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting)”. There were no entities found to be conducting financial leasing activities subsequent to these regulatory changes. Accordingly, three lending entities registered with the Authority during the review period. This sector is an insignificant contributor to the economy and offers small loans, which typically range between $500 and $5,000, but not exceeding $25,000.

Assessment of Sectoral ML Threats

The Lending sector has a LOW inherent ML threat rating. The sector was not assessed in 2017, as it had not yet been brought into scope under the AML regime. There are only 3 operators in this lending sector. These businesses operate as micro-lenders, with limits on the size of the loans and a business model for profit maximisation which militates against quick turnaround loans, which could be used for laundering. In addition, there was no intelligence or other information in the 2020 assessment related to any criminal activity within this sector involving ML.

Back to Table of Contents

Analysis of Sector Inherent ML Vulnerabilities

The inherent ML vulnerability rating for the Lending sector was MEDIUM-LOW. This rating was based on several sectoral features. First, as noted above, there were a total of three registered lending entities during the review period. Product range is also limited. There are two types of loans offered within the sector currently: small personal loans (similar to "pay-day loans") and larger collateralised loans. In addition, the use of agents within the sector is not permitted. Ratings for other key vulnerability factors within the sector were focused on the areas listed below:

Size

The total size of the sector was rated as EXTREMELY LOW, especially when compared to the rest of the financial sector. In light of the size of the sector, and its coming within scope relatively recently, a data collection regime to confirm the volume of business was still in development. However, in discussions with participant companies during the assessment, it was noted that transaction limits for small personal loans were very small in value (i.e. less than $3,000) and even though collateralised loans could be as large as $10k, very few of such loans have been issued to date.

Client Base

The sector's client base profile was rated as LOW vulnerability. The market for this sector comprises local residents. It is perceived that there may be a tranche of local residents who may be underserved by the banks or who choose not to use the banks, often for cost reasons, leading to a market niche for this sector. It has been observed, even at these early stages of development of the sector, that staff turn away clients that they deem as suspicious, indicating a degree of awareness, training and effectiveness by the sector towards ML.

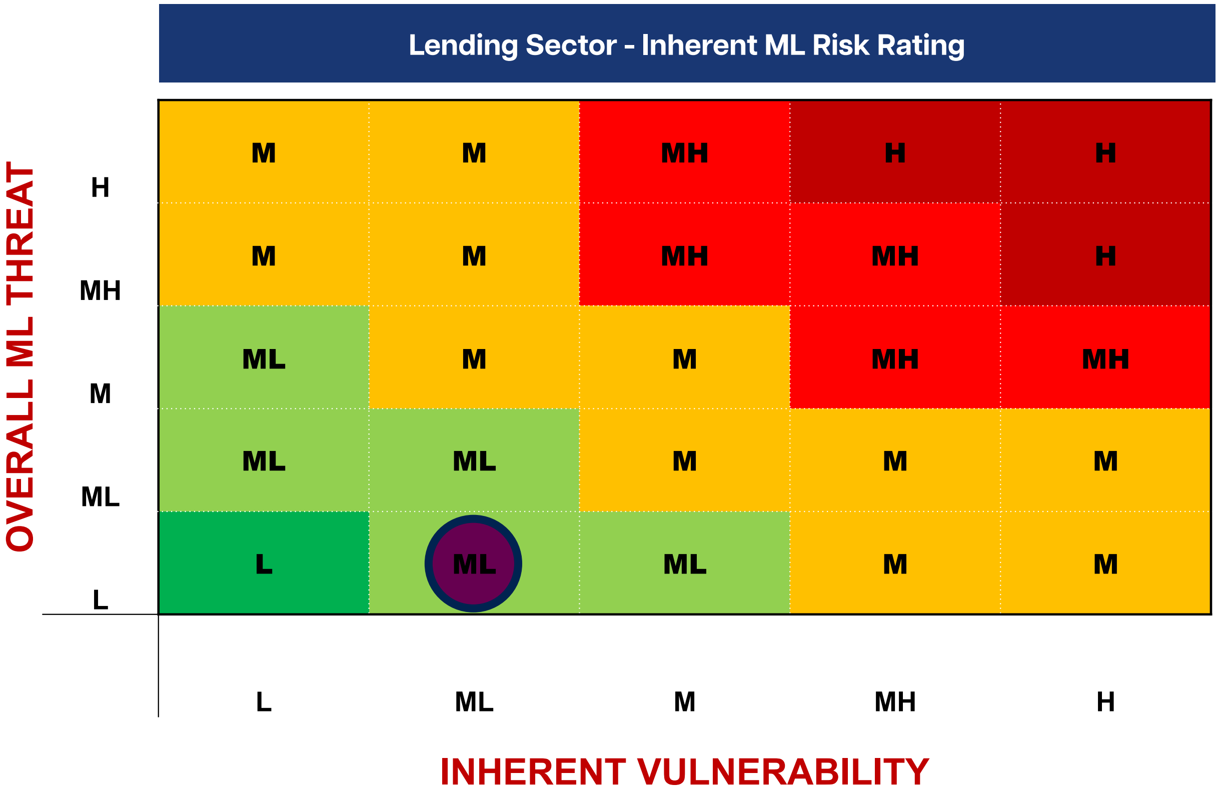
Cash Activity and Frequency of International Transactions

The level of cash activity is assessed as HIGH, and the frequency of international transactions is assessed as low. The lending sector is a cash-intensive business, however due to the entirely domestic nature of the clients, there are almost never any international payments. Additionally, all business is conducted face-to-face, removing risks associated with anonymous use of the sector's products. It is acknowledged that the cash-intensive nature of the business activity within the sector, may make tracing transactions difficult as the source and use of funds can be concealed.

Back to Table of Contents

Conclusion

The heat map below summarises that the Lending sector has a LOW ML threat rating, and when combined with the inherent vulnerability rating of MEDIUM-LOW, the ML risk rating is MEDIUM-LOW.



Lending Sector - Inherent ML Risk Rating

OVERALL ML THREAT					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

INHERENT VULNERABILITY

Back to Table of Contents

Chapter 11: Bermuda Stock Exchange (BSX)

Summary of Findings: The inherent ML risk rating for the BSX remains MEDIUM-LOW. This rating is derived from the medium-low rating for the BSX's inherent vulnerability and low rating for ML threats. The public nature and transparency of the BSX; its electronic trading, settlement and depository platform; and profile of trading members, who are all fully licensed and regulated institutions, continue to support this rating.

AML/ATF Supervisory Authority – Bermuda Monetary Authority

Introduction

The Bermuda Stock Exchange (BSX) is a Recognised Investment Exchange under the Investment Business Act 2003 and operates as a Regulator in its own right, subject to oversight by the Bermuda Monetary Authority. The BSX has been in operation since 1971 and is Bermuda's only Stock Exchange. As a full member of the World Federation of Exchanges, and affiliate member of the International Organisation of Securities Commissions the BSX is globally recognised. The BSX is the world's largest offshore, fully electronic securities market offering a full range of listing and trading opportunities for international and domestic issuers of equity, debt, depository receipts, insurance-linked securities (ILS) and derivative warrants[22]. The ILS market continued its growth from 61 new ILS listings in 2016 to 155 in 2019, bringing the total of listed ILS securities to 401 by the end of 2019, with a combined nominal value of $34.72 billion.[23] Bermuda remained the leading jurisdiction for listings of ILS. A Stock Exchange is typically characterised by the speed in execution of transaction and global reach, providing some exposure to ML/TF. However, the transparency required from listed entities and the public nature of the BSX makes it less attractive to criminals, who typically prefer more opaque vehicles.

Assessment of Sectoral ML Threats

The Bermuda Stock Exchange retained its rating of LOW ML threat for the same reasons as in 2017 – namely that its activities, products and services make it unattractive for criminals for ML; there are also significant barriers to entry to the sector.

Analysis of Sector Inherent ML Vulnerabilities

The BSX's inherent ML vulnerability rating was MEDIUM-LOW. The total market capitalisation of the BSX decreased from approximately $344 Billion in 2016[24] to approximately $332 Billion[25] in 2019. The total domestic trading volume of BSX was 3.1 million shares, with a corresponding value of $30.6 million,[26] down from $49.7 million[27] in 2018. This highlights the comparatively small scale of the domestic trading

[22] https://www.conyers.com/wp-content/uploads/2018/06/Pub_BDA_The_Bermuda_Stock_Exchange.pdf

[23] BSX, End of Year Review 2019

[24] BMA, *Annual Report*, 2016

[25] BSX, End of Year Review 2019

[26] BMA, *Annual Report*, 2019

[27] BMA, *Annual Report*, 2019

Back to Table of Contents

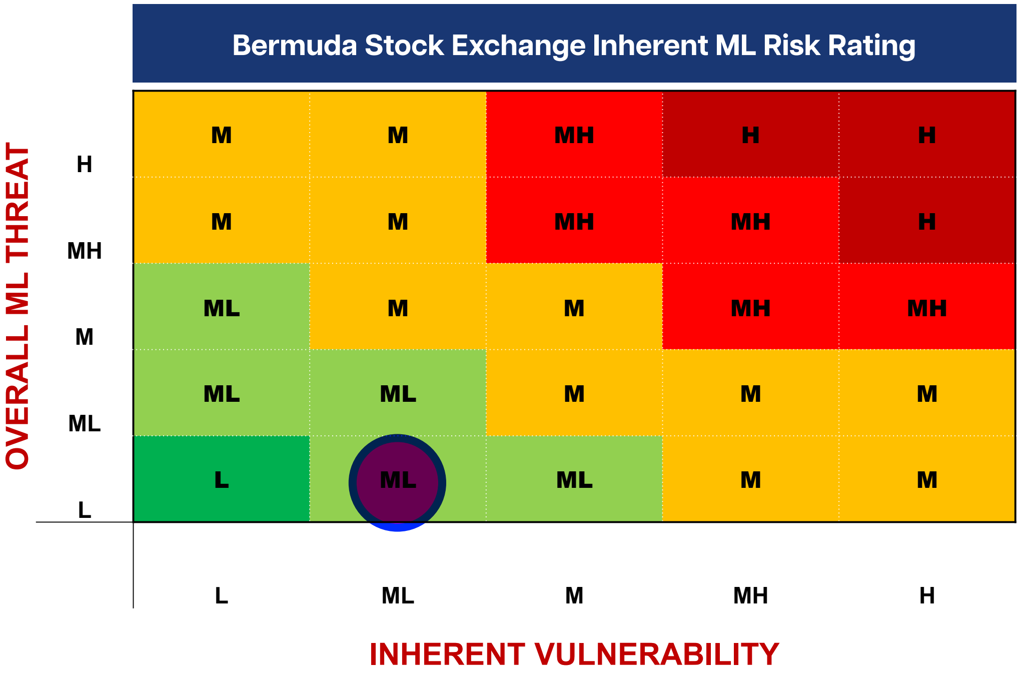
activity conducted on BSX. With a market capitalization of $332 billion, the BSX is significantly smaller than the New York Stock Exchange (NYSE) and the London Stock Exchange (LSE), with market capitalization of $22.9 Trillion and $3.8 Trillion respectively. The BSX's stock market turnover ratio in 2019 was ranked 68th out of 71, at 0.77%, compared to the world average of 27.04%[28]. Such a relatively low market turnover ratio continued to limit the BSX's ML vulnerability.

Similarly, the institutional and highly regulated nature of the BSXs client base, i.e. trading members, was rated as medium risk. All agents in this sector are also regulated institutions, who must adhere to established financial reporting and operational standards. Trading members are all licensed entities fully regulated by the BMA. Listed entities must have been proposed by a listing agent, who must be approved by the BSX, and have been listed via a predominantly face-to-face process.

Further, the international cooperation and high transparency requirements related to public companies and the BSX's fully-automated electronic trading platform diminish its exposure to ML. The BSX's electronic trading, settlement and depository platform is licensed, and specifically designed to support the secondary market trading and settlement of sophisticated listed securities. The platform allows for the trading of both equity and fixed income securities in a modern and secure environment. All listed securities are supported through Bloomberg (BSX <GO>) and the BSX web site www.bsx.com carries details on all listed securities, providing important information supporting transparency and disclosure. Overall, the vulnerability of this sector therefore relates primarily to the frequency of international transactions (>95% of all transactions) and risks related to ILS.

Conclusion

As shown in the heat map below, the overall ML risk rating for the BSX remains MEDIUM-LOW. This rating is derived from the MEDIUM-LOW rating for the BSX's inherent vulnerability and LOW rating for ML threats.



Bermuda Stock Exchange Inherent ML Risk Rating

OVERALL ML THREAT					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

INHERENT VULNERABILITY

[28] Global Economy, Country rankings of stock market turnover ratio

Back to Table of Contents

Chapter 12: Trust Service Providers (TSPs)

Summary Findings: The ML threat for the Trust Service Provider (TSP) sector was assessed to be HIGH, and this, together with the inherent vulnerability sectoral rating of high, resulted in an inherent risk rating for the TSP sector of high. This is due to sectoral characteristics common to the industry globally, e.g. the high value of asset risk transfers, global reach of trusts under operation and related risk profile of customers such as high-net-worth individuals and PEPs.

AML/ATF Supervisory Authority – Bermuda Monetary Authority

Introduction

As of 2019, Bermuda's trust sector had 28 Licensed Trust Companies (or Trust Service Providers, TSPs). Bermuda's primary statute governing the regulation of trust business is the Trusts (Regulation of Trust Business) Act 2001. Trusts are administered by trustees who have the power to manage, employ or dispose of the assets in accordance with the terms of the trust deed and the special duties imposed upon them by law. The number of trusts must be reported to the BMA by those TSPs that are licensed or applying for an exemption from licensing. All trustees who offer their service for a fee are subject to AML/ATF regulation.

The focus of this analysis is on the AML/ATF regulated Trust Service Provider sector, which includes Licensed Trust Companies and Private Trust Companies (PTCs). For this sector, the market emphasis is on offering trust services to High Net Worth families or Individuals.

Private trust companies are exempt from the licensing regime of the *Trusts (Regulation of Trust Business) Act 2001*. Other trustees may be exempt if they meet the requirements of the *Trusts (Regulation of Trust Business) Exemption Order 2002*. However, although PTC structures are exempt from licensing, they are still covered under AML/ATF regulations, either through a relationship with a TSP or through direct registration with the BMA as a non-licensed person.

Assessment of Sectoral ML Threats

The ML threat rating for the TSP sector was HIGH, driven by a number of factors. In many of the SARs filed by the sector during the review period, suspected foreign tax crimes and fraud featured significantly. In particular, law enforcement reported that domestic authorities provided assistance in a large-scale investigation overseas, in which a foreign national was suspected of having laundered over $1.9 billion using a local PTC to evade taxes, with some evidence of complicity on the part of this PTC. Also, Bermuda received criminal tax information requests from overseas counterparts related to foreign crimes impacting Bermuda's trust sector in 2017 and 2018.[29] There were no domestic ML investigations based on locally-generated proceeds of crime during the period.

[29] A total of 5 criminal tax information requests were received in 2017 by Bermuda; 65 were received in 2018; and 23 in 2019. Due to confidentiality restrictions imposed by the OECD's Global Forum on tax authorities, only limited information could be shared during the NRA. It is therefore unclear how many of the requests specifically related to this or any of the affected sectors in each year.

Back to Table of Contents

Overall, the ML threat from internationally-sourced business remains higher than from local clients within the sector. In light of this, and other contributing factors such as the sector potentially being targeted for ML purposes from foreign tax crimes, the ML threat was deemed to be high.

Analysis of Sector Inherent ML Vulnerabilities

The TSP sector's inherent ML vulnerability rating was HIGH. Globally, it has been demonstrated that TSPs can be attractive to criminals given their key role as trustees, administrators and intermediaries that manage the financial affairs of the wealthy. PTCs in particular, have typically been used for tax evasion purposes.

There are not many cases prosecuted in Bermuda related to abuse of the trust sector for ML purposes. However, it is recognised that Bermuda's client base profile for trust products and PTCs remains high risk, given that clients are largely high net worth individuals and PEPs, both resident and from overseas. Also, Bermuda features sectoral characteristics common to the industry globally, e.g. the high dollar value of trusts managed in the sector, and the global reach of trusts under operation.

There is also the potential that trust vehicles may be used for ML purposes. As such, the 2020 NRA applied a granular approach in its analysis, assessing five broad categories of trust products administered by Licensed Trust Companies shown in the table below.

Table 4: Vulnerability Ratings for Various Types of Trust Products

Sector	Sub-sector	Vulnerability Rating
Trusts	Discretionary Trusts	HIGH
	Fixed Interest Trusts	MEDIUM
	Purpose Trusts	MEDIUM-HIGH
	Charitable Trusts	MEDIUM-HIGH
	Employee Benefit Trust	MEDIUM-HIGH
	Other Trusts (Unit Trusts, PTCs)	HIGH

Back to Table of Contents

Overall, discretionary trusts, purpose trusts and PTCs were assessed as generally higher risk areas in the sector:

i. **Discretionary Trusts**

Discretionary Trusts are the most commonly established form of Trust in Bermuda and rated as having a HIGH inherent ML vulnerability. (33% of total Asset under Administration at approximately $39 billion). There were approximately 1,587 Discretionary Trust client relationships with a Bermuda licensed trustee as of 2019. Within a Discretionary Trust, the beneficiaries have no legal right to the property of the trust. The trust deed confers a wide power on the trustees to act at their discretion for the benefit of any one or more of the beneficiaries. This is in clear contrast to a Fixed Interest Trust, in which the interests of the beneficiaries are clearly quantified and restricted. The Discretionary Trust service, given its size and dominance within the Trust sector, drives much of the sector's client profile, which primarily includes foreign-based HNWIs, from multiple jurisdictions. The vulnerability for Discretionary Trusts is somewhat mitigated because the licensed trustee has final discretion on the distribution of funds out of the trust structure. If the trustee has any reason to be suspicious regarding a transaction, they are not obligated to transfer any funds.

ii. **Purpose Trusts**

Purpose trusts have a MEDIUM-HIGH inherent vulnerability rating. Purpose Trusts are created to fulfil specific purposes rather than hold property for beneficiaries and were introduced under the Trusts (Special Provisions) Amendment Act 1998. In addition to commercial use, a purpose trust is commonly used for philanthropic and estate planning purposes. Purpose Trusts represent approximately $23 Billion of Assets under Administration, which is 20% of the sector. In 2019 there were approximately 486 Purpose Trust clients with licensed trust companies. Purpose Trusts also have a large international client profile, predominantly HNWIs.

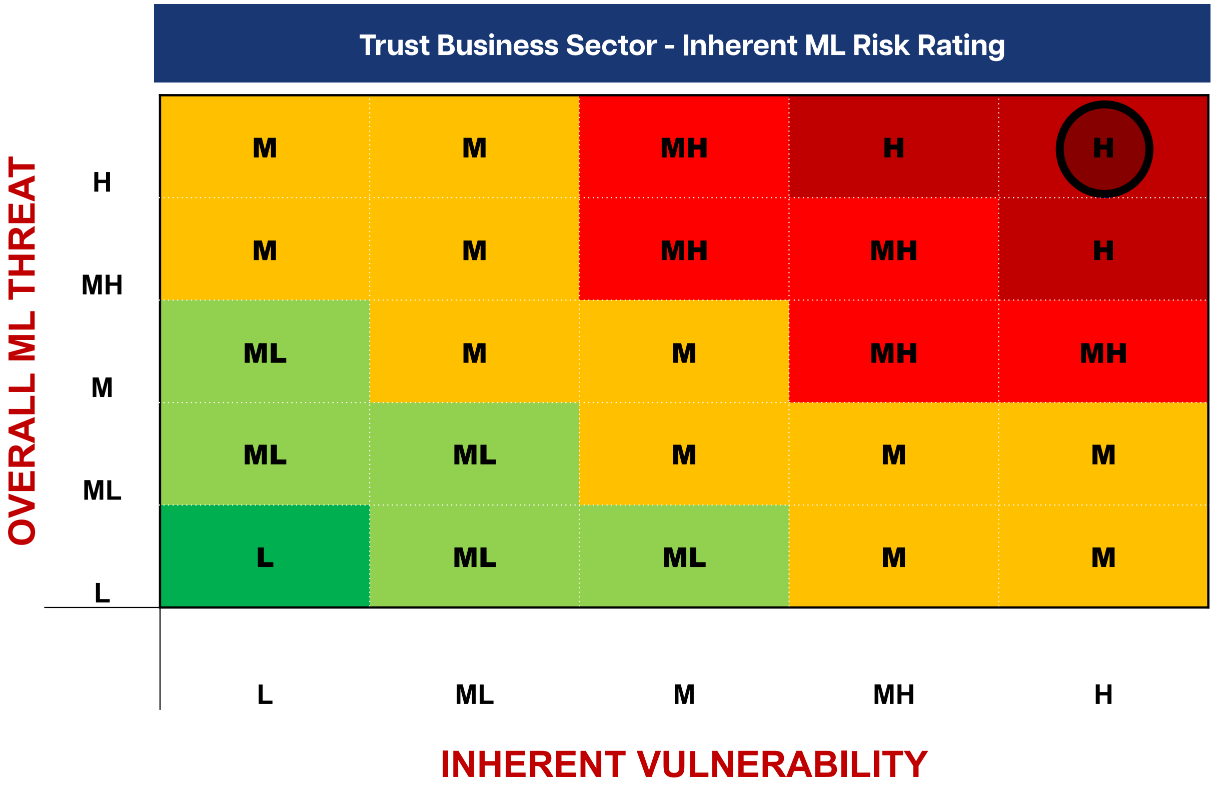
iii. **Private Trust Companies**

PTCs have a HIGH inherent vulnerability. These are companies with a largely international client base, whose sole purpose is to act as trustees for specific trusts or a closely related group of trusts. PTCs account for $39 billion of Assets under Administration, which is 33% of the sector. The high inherent vulnerability rating remains partly driven by the lack of information in this sub-sector and limited direct oversight.

Back to Table of Contents

Conclusion

As shown in the heat map below, the ML threat for the Trust Service Provider (TSP) sector was assessed to be HIGH, and this, together with the inherent vulnerability sectoral rating of high, resulted in an overall risk rating for the TSP sector of HIGH.



Trust Business Sector - Inherent ML Risk Rating

OVERALL ML THREAT	L	ML	M	MH	H
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M

INHERENT VULNERABILITY

Back to Table of Contents

Chapter 13: Corporate Service Providers (CSPs)

Summary Findings: The inherent ML risk rating for the CSP sector is HIGH, based on an average MEDIUM-HIGH rating for inherent vulnerability of their products and services, and the high rating for ML threats. The rating reflects in part the CSPs' role in Bermuda's gatekeeping, given their function in legal person formations for business entering the jurisdiction; their international client base; the large number of companies being managed; and the complexity of international transactions conducted within the sector.

AML/ATF Supervisory Authority – Bermuda Monetary Authority

Introduction

The CSP sector has matured significantly since the last ML NRA in 2017, as the sector is now fully regulated. This sector is sizable based on both the number of licensed providers and their domestic and international customer base. As of the end of 2019, there were 95 CSPs servicing a total of approximately 12,000 customers. The scope of analysis in the 2020 NRA for the sector was considerably deepened compared to 2017. In 2017, CSPs were not yet regulated and no product data was available, therefore the assessment reviewed the sector as a whole. As a result, the sector's inherent vulnerability assessment was based on the types of licences issued. The 2020 NRA, represents a detailed product and service analysis, allowing for more granular detail in the inherent vulnerability assessment, as guided by the FATF recommendations.

The term "CSP business" is defined as the provision of corporate services[30] for profit, such as acting as a company formation agent, providing nominee services, providing administrative and secretarial services, or the performance of functions in the capacity of resident representative.

There are two classes of licence for CSPs in Bermuda: Unlimited and Limited. An unlimited licence permits the CSP to form a company without seeking permission from the Controller of Exchange, whereas such permission is required in the case of limited licences. Currently there are no unlimited licences in issue.

Assessment of Sectoral ML Threats

The ML threat rating for the CSP sector is HIGH. This rating is higher than 2017, based on the enhanced understanding of the sector subsequent to implementing AML/ATF supervision. The level of foreign investigation requests Bermuda's FIA received from overseas counterparts related to the sector also underpinned this rating. It is also believed that the scale of undetected criminal proceeds related to CSPs may have previously been underestimated; there is now increased access to data on the sector in line with the increased AML/ATF oversight in place. There were 70 SARs filed by the sector and 9 STRs during the review period. This aligns with the sector's business model, being less transactional in nature and more administrative. Given the value of the businesses administered by CSPs, and that they are a major gateway for international interests into Bermuda's international financial services market, the sector is potentially exposed to a higher scale of ML than many other sectors. Based on the sector's international client base, there is ML threat exposure from foreign sources, in particular related to tax evasion, fraud, corruption and market manipulation/insider trading. Therefore, the ML threat to this sector is High.

[30] Please refer to Section 2(2) of the Corporate Service Provider Business Act for a comprehensive list of services falling under the Act.

Back to Table of Contents

Analysis of Sector Inherent ML Vulnerabilities

The CSP sector's inherent ML vulnerability rating is MEDIUM-HIGH. In 2020, a more granular product assessment was performed, which is the foundation of the inherent vulnerability rating. For the purposes of assessing product risk, 11 services within the sector were identified and assessed. Based on the assessment, key components of focus were the client base and the higher risk services.

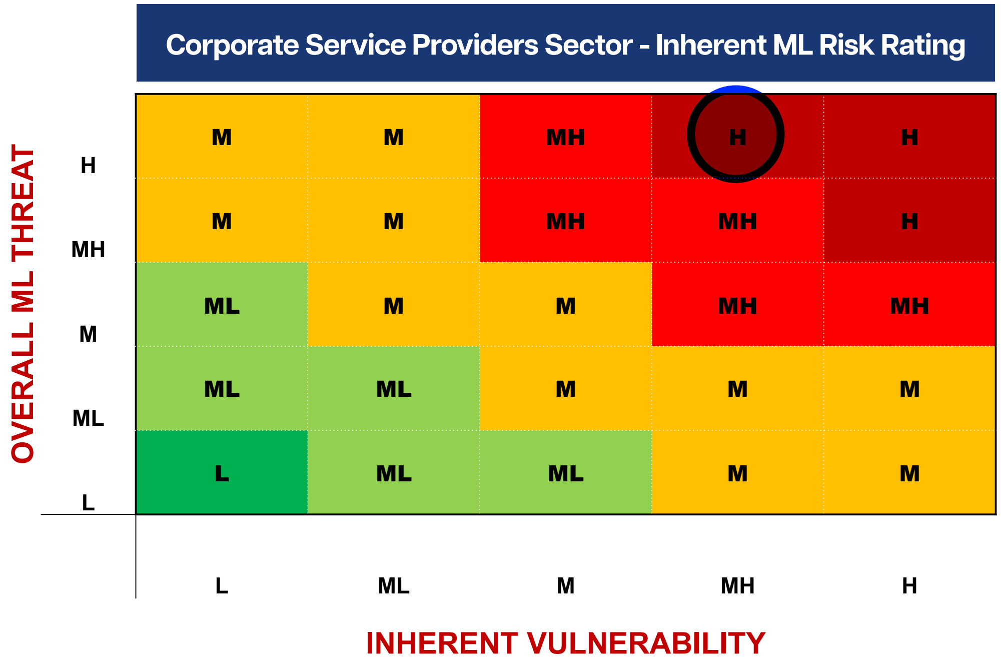
Bermuda's CSP sector ML vulnerability reflects the higher risk factors common to jurisdictions globally, as summarised below:

- The client profile of Bermuda's CSP sector is perceived as high vulnerability, given CSPs service a range of legal person entities, often with complex corporate structures, with beneficial owners who may be HNWIs based in higher-risk jurisdictions and/or in higher-risk industries.
- A number of CSP products or services presented higher vulnerability, specifically:
  - Acting as a Formation Agent;
  - Nominee Services;
  - Acting as or Fulfilling the Function of Director & Officer, Secretary; and
  - Providing a Registered Office.

CSPs continue to be regarded as having high vulnerability to ML risk. The CSP would either be introducing parties to the country or maintaining records via these services, and potentially could be used either knowingly or unwittingly by bad actors to facilitate ML activity. CSPs also facilitate establishing companies, opening bank accounts, and setting up other legal structures that could be misused by criminals for ML activity.

Conclusion

The inherent ML risk rating for the CSP sector is HIGH, based on the MEDIUM-HIGH rating for inherent vulnerability, and the HIGH rating for ML threats, as shown in the heat map below.



Corporate Service Providers Sector - Inherent ML Risk Rating

OVERALL ML THREAT					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

INHERENT VULNERABILITY

Back to Table of Contents

Chapter 14: The Legal Sector

Summary Findings: The inherent ML risk rating for the sector is HIGH. This was based on the sector's MEDIUM-HIGH rating for inherent sectoral vulnerabilities, as it was in 2017, together with the high rating for ML threats. The ML risk rating is the same as in 2017.

AML/ATF Supervisor – Barristers and Accountants AML/ATF Board

Introduction

As of December 2019, there were 69 law firms registered with the Barristers and Accountants AML/ATF Board ("the Board"). Of that number, 30 firms were categorised as Regulated Professional Firms (RPF) subject to AML/TF requirements, on the basis that they provide "specified activities' as defined in the Proceeds of Crime Act 1997._

The relevant services the sector offered in this regard were real estate transactions; as well as services relating to organising, creating, operating and managing legal entities, and their funding; and management of financial assets.

The sector has reported that in some cases, Corporate Services Providers (CSP) affiliated to law firms were providing incorporation services but operating as separate legal entities. It was also noted that the demarcation lines between some law firms and their affiliated CSPs appeared to be blurred, and separate risk profiling assessments of law firms and CSP operations were needed under their respective compliance regimes. Accordingly, with the aim of ensuring that transactions affiliated CSPs conduct can be fully monitored, Rule 7 of the Bermuda Bar (Barristers and Accountants AML/ATF Board) Rules 2018 was established. This requires all law firms with a turnover of more than $250,000, or whose affiliated corporate services business constitutes more than 10% of their business, to transfer to and operate the CSP aspect of their business by a separate incorporated affiliate. The Board and the Bermuda Monetary Authority have agreed to jointly supervise legal firms who also operate separate affiliated CSPs.

Assessment of Sectoral ML Threats

The ML threat rating for this sector was increased to high in 2020, compared to the rating of MEDIUM-HIGH in 2017. The 2017 rating balanced ML threats of the sector's specified activities with its ML threat exposure from affiliated CSP business (rated high) and the real estate sector (rated medium-low).

In 2020 the spectrum of ML-related intelligence and investigations involving this sector increased. This included a significant case involving a bad actor within the sector facilitating ML through real estate transfers to assist local drug traffickers. Another case involved a local lawyer acting as trustee for a PTC which was one of the subjects in a $1.9 billion tax evasion/fraud/ML investigation, in which the local authorities provided investigative assistance to the USA. These investigations and the associated intelligence contributed to the increased threat rating of high, and also motivated higher ML threat considerations for the sector's real estate business.

From the 15 SARs and 6 STR filings the sector submitted in the review period, areas for suspicion related to forming corporate structures for issuing crypto-currency, initial coin offerings and tokens; clients in high-risk foreign jurisdictions; scams involving cheque fraud; and tax evasion.

Back to Table of Contents

Analysis of Sector Inherent Vulnerabilities

The legal sector's inherent ML vulnerability rating was MEDIUM-HIGH. Globally, the legal profession is viewed as providing services that can either be a gateway into the financial system, or facilitate anonymity in ownership and control structures, which potentially obscures the identity of individuals conducting complex money laundering schemes. Accordingly, it is imperative to analyse the sector periodically, to identify whether any of its inherent features expose it to vulnerability for misuse by criminals.

Bermuda's 2020 NRA examined a range of the legal sector's features that could be inherent ML vulnerabilities, including total size/business volume, the nature of clientele, product/service offerings and payment mechanisms. The key areas examined and rated are described below:

Total size/volume

The total size of the sector was rated as medium. The assessment of this inherent vulnerability factor focused on the total number of RPFs conducting specified activities, which was 30 in 2020, up from 23 in 2019. The results also indicated a growing number of law firms conducting real estate transactions during the review period and this, coupled with the high cost of real property in Bermuda, increased the inherent vulnerability rating.

Client base

The sector's client base profile was rated as high, increased from 2017. The sector's clientele includes local and foreign PEPs, HNWIs; non-resident clients, including from high-risk jurisdictions; and clients that have ownership in complex legal structures. However, CSPs conduct the bulk of specified activities in this category, and they now fall within scope of the increased monitoring and supervision of affiliated CSPs dealing with such business established under Rule 7 of the Bermuda Bar (Barristers and Accountants AML/ATF Board) Rules 2018.

Level of cash activity

The level of cash activity associated with the profession remained low. All RPFs reported that they either had a “no cash” policy in place or a low cash threshold limit.

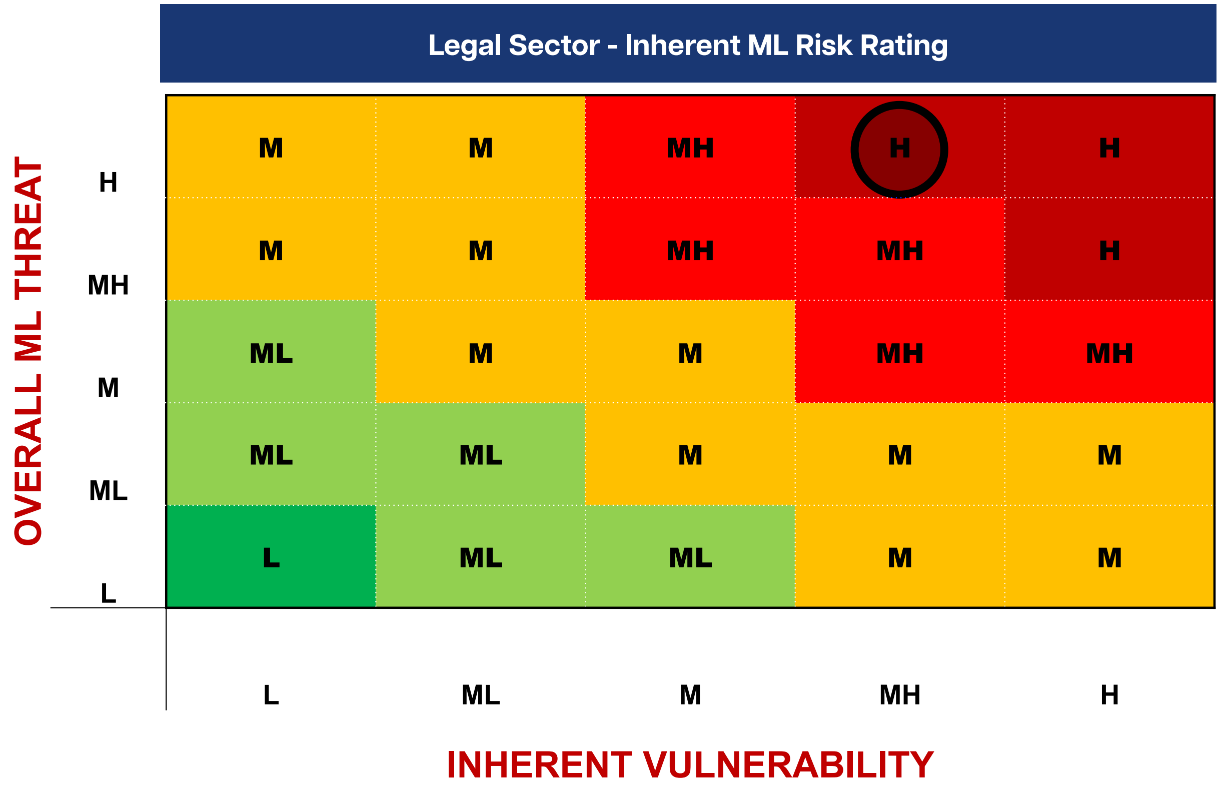
Products and Services

This vulnerability factor was assessed for the first time in 2020 and rated as medium-low. Key services in this area include buying and selling real estate, services relating to organising, creating, operating and managing legal entities and managing financial assets (money, bank accounts, securities, etc.) While real estate transactions, managing client money and anything involving the flow of funds are considered to be higher risk areas, the RPFs reported that a firm has control of clients' bank accounts only on very rare occasions. In the majority of cases this is usually in the hands of a CSP. The RPFs also reported that in every circumstance real estate purchases are a non-cash transaction.

Back to Table of Contents

Conclusion

As shown in the heat map below, the inherent ML risk rating for the sector is HIGH, the result of the MEDIUM-HIGH rating for inherent vulnerabilities, together with the high rating for ML threats.



Legal Sector - Inherent ML Risk Rating

OVERALL ML THREAT					
H	M	M	MH	[✓ H]	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

INHERENT VULNERABILITY

Back to Table of Contents

Chapter 15: The Accounting Sector

Summary Findings: The Accounting Sector's inherent vulnerability rating was MEDIUM-LOW, and the ML threat for the sector was rated as low, resulting in an ML risk rating of MEDIUM-LOW. This ML risk rating is the same as in 2017.

AML/ATF Supervisor – Barristers and Accountants AML/ATF Board

Introduction

As of December 2019, the accounting sector comprised 8 firms registered with the Barristers & Accountants AML/ATF Board. All of these firms are classified by the Board as Regulated Professional Firms (RPF) and are subject to AML/ATF requirements, on the basis that they provide "specified activities", as defined in the Proceeds of Crime Act 1997. There were a total of 1186 Chartered Professional Accountants employed by these firms as of December 2019.

The key services the sector offers in this context relate to liquidation and receivership services, advisory work, audit, assurance and tax services.

Assessment of Sectoral ML Threats

The Accounting sector retained a LOW ML threat rating in 2020. This rating is driven by the fact that the majority of firms in the sector are affiliated with international accounting firms, and their primary business remains auditing. Also, there are distinct firewalls separating their audit business from the business that their affiliated CSPs conduct. Very few SARs were received from this sector, but they were primarily based on findings in their audit practice.

Analysis of Sector Inherent Vulnerabilities

The Accounting sector's inherent ML vulnerability was assessed as being MEDIUM-LOW. The assessment examined a range of sectoral features that could be inherent ML vulnerabilities, including the total size/business volume of the profession; its client base profile; products and services provided; payment mechanisms; and frequency of international transactions. The key areas examined and rated are described below:

Total size/volume

The total size/volume of the Accounting sector was rated as medium-low. Number of Providers: All 8 accounting firms in the sector are RPFs registered with the AML/ATF Board. However only a few of the services they provide are classified as "specified activities" as defined in the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008, specifically, liquidation and receivership services.

Client Base

The sector's client base profile was rated as medium. This variable assessed the nature and geographic location of the sector's clients, e.g. whether the client base includes any local or foreign PEPs, or persons with high net worth; whether there are non-resi-

Back to Table of Contents

dent clients, including from high risk jurisdictions, whether clients are legal persons or have ownership in complex legal structures.

Although there is a potential for high-risk clientele in this sector, the assessment results indicated that firms have a small number of medium or high-risk clients. The firms reported that all overseas clients are subject to rigid due diligence and onboarding procedures. Also, 7 out of the 8 firms had zero transactions with high-risk ML jurisdictions, with the remaining one having five or fewer transactions in a year.

Level of cash activity

The level of cash activity associated with the sector was rated as low. All firms reported that they either had “no cash” policies in place, to preclude the receipt of cash in their operations; or that they implement a low cash threshold limit within their practice.

Products and Services

The products and services the sector offers were rated as MEDIUM-LOW. The key services firms offer that classify as “specified activities” relate to liquidation and receivership, advisory work, audit, assurance and tax services. For the 8 RPFs in this sector:

- 1 firm did not conduct specified activities as defined by section 49(5) of the Proceeds of Crime Act 2008.
- 4 firms conduct few transactions related to specified activities; the majority of those transactions relate to liquidation services connected to them acting as Court-appointed liquidators.
- 1 firm has a licenced Corporate Service Provider and a licenced Trust Company (which are separate legal entities), which conducted specified activities all monitored under the Bermuda Monetary Authority.
- 2 firms reported having a few clients for whom they perform bookkeeping and ancillary services. These firms reported that the revenue generated from these clients is very low, and many of the transactions relate to payment of personal living expenses, small business bookkeeping and bill payments.

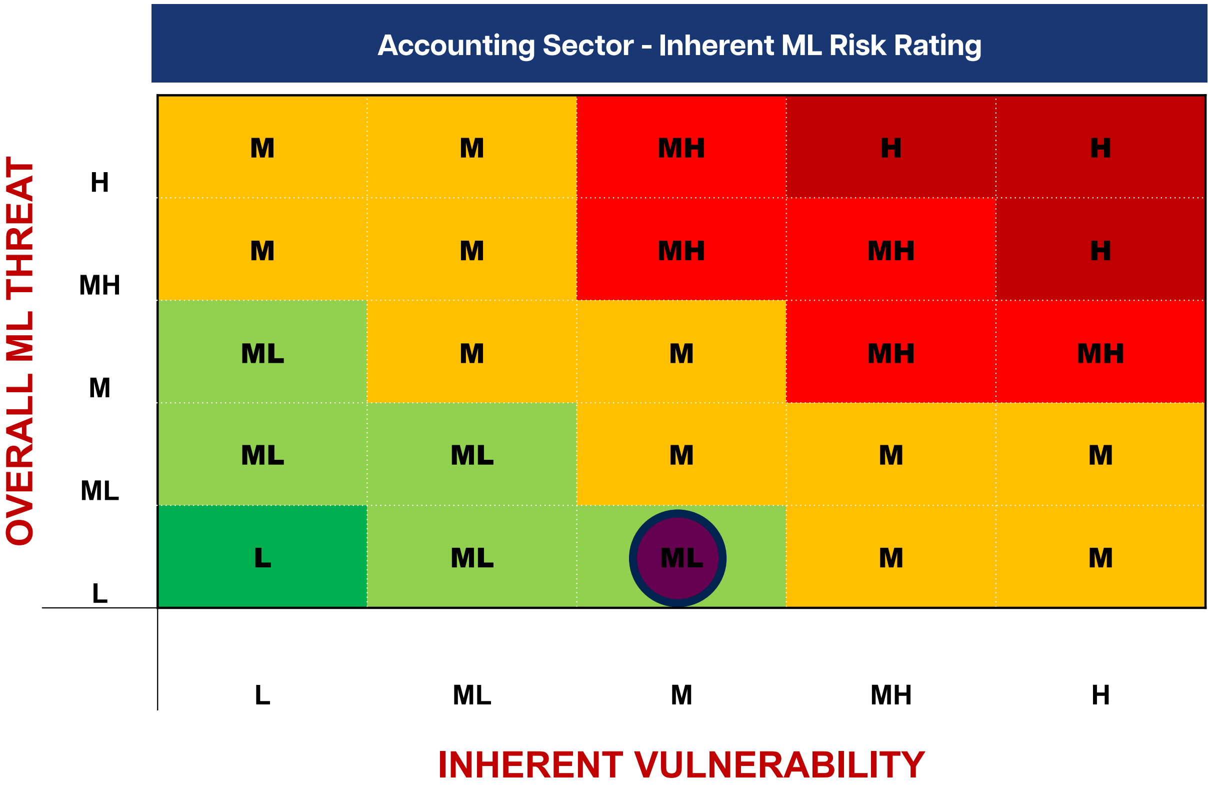
Other Vulnerability Factors

The assessment reinforced the fact that accountants can be retained on matters which could bring them within the scope of mainstream financial services. However, such services are often conducted under the affiliate CSP corporate entity, which falls within the supervisory regime of the Board. Firms reported low engagement in other vulnerability factors, such as using intermediaries/agents and non-face-to-face transactions. Discussions with CPA Bermuda also confirmed that the use of accounting firms in tax/fraud schemes does not exist as there is a low demand for tax advice in Bermuda. In 2019, CPA Bermuda developed a standardised system to assist in identifying “regulated activities”. The only tax service identified related to compliance with payroll tax.

Back to Table of Contents

Conclusion

As shown in the heat map below, the Accounting Sector's inherent vulnerability rating was MEDIUM-LOW, and the ML threat for the sector was rated as low, resulting in an inherent ML risk rating of MEDIUM-LOW. This ML risk rating is the same as in 2017.



Accounting Sector - Inherent ML Risk Rating

OVERALL ML THREAT					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

Back to Table of Contents

Chapter 16: The Real Estate Sector

Summary Findings: The ML risk rating for Bermuda's real estate sector is MEDIUM-HIGH. This is based on an unchanged inherent ML vulnerability rating of MEDIUM-HIGH, whilst the ML threat rating has moved to medium, from the previous MEDIUM-LOW rating in 2017.

AML/ATF Supervisory Authority – Superintendent of Real Estate

Introduction

As at 31 December 2019, the real estate sector comprised 51 licensed brokers and 217 licensed agents. There are two major real estate firms operating on the island who provide full-scale services, i.e. residential and commercial real estate sales, land and valuation surveying, property management, residential rentals, relocation services, commercial leasing and auctioneering. The majority of firms are considered small to medium-sized sole proprietorship operators that focus on rentals and engage in residential and commercial sales. Real estate firms have a diverse clientele including trustees, and both domestic and international individuals. The purchase of real estate in Bermuda is not a cash-based activity and there are firm policies restricting the use of cash for real estate transactions.

The sale of real estate was valued at $282,196,456 in 2019 according to statistics provided by the Land Title Registry. This figure represents sales and purchases by Bermudians (71% of total sales), non-residents (6.3%), non-residents of fractional properties (21%) and local trusts (1.4%).

The sector (including real estate rentals) represented 15.1 percent of GDP in 2019 with $972,485 million in output compared to $953,742 million in output in 2018 (Revised). The increase is attributable to an uptake in real estate activities with leased property.

Assessment of Sectoral ML Threats

The 2020 NRA increased the ML threat rating for Bermuda's real estate sector to MEDIUM, from MEDIUM-LOW in 2017. The 2017 rating was driven primarily by severe losses in real estate value and the prolonged slow pace of local sales in the post-2008/09 recession environment. That was also coupled with stringent conditions preventing foreigners from readily accessing the local real estate market. These factors reduced the scale of potential local- and foreign-sourced ML threat to the sector

However, a significant factor in the 2020 assessment were the cases currently under investigation and the potential new methods being used by a bad actor in the legal sector, to facilitate ML in the real estate market on behalf of local drug traffickers. In light of this, and given emerging reports involving that bad actor, a higher rating of Medium was considered justified. Therefore, the heightened ML threat to this sector was driven by a participant in the legal sector and no licensed real estate brokers were identified as being involved in this activity.

Analysis of Sector Inherent Vulnerabilities

The real estate sector's inherent vulnerability to money laundering was rated as MEDIUM-HIGH. The inherent sectoral features assessed to determine ML vulnerability included the size of transactions in the sector, the type of clientele (local and international purchasers) and payment mechanisms, among others.

Back to Table of Contents

Size of transactions

Although not as large as the financial services industry, with total sales valued at $282,196,456 in 2019, the size of transactions in the sector potentially provide an opportunity for large sums of money to be laundered.

Client Base

The sector's client base profile is rated as medium. This is driven by the presence of non-Bermudians (also referred to as restricted persons), PEPs and HNWIs among Bermuda real estate clientele. Despite related immigration controls, in 2019 the dollar value of international transactions in the sector represented 27.3% of the total value of sales transactions, vs. 76.2% of domestic transactions. These non-Bermudian purchasers originated primarily from the United States, the United Kingdom, and Canada. Although most of these countries have implemented AML/CFT regimes, some jurisdictions impose weaker beneficial ownership requirements, which contributes to moderate ML vulnerabilities.

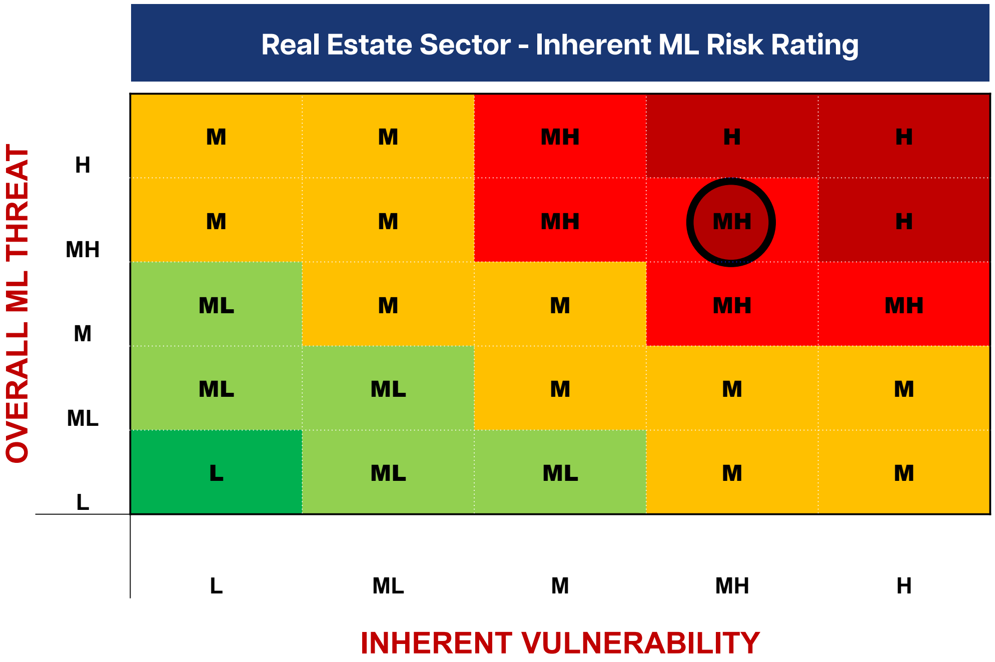
Other vulnerability factors

Other general factors contributing to the medium-high inherent vulnerability rating involve the use of agents, difficulty in tracing the transaction records (e.g. trusts), use of the business in fraud or tax evasion schemes and the frequency of international transactions in the real estate sector. Anonymous and non-face-to-face use of the products also remains a vulnerability for transactions involving trusts.

In addition to these vulnerabilities, the Bermuda Police Service indicated that they were aware of a real estate professional who is the subject of a pending money laundering investigation. The allegations in this matter may reveal further vulnerabilities in the sector not previously contemplated.

Conclusion

As shown in the heat map below, the inherent ML risk rating for the real estate sector is MEDIUM-HIGH, based on an inherent vulnerability rating of MEDIUM-HIGH and a ML threat rating of MEDIUM.



Real Estate Sector - Inherent ML Risk Rating

OVERALL ML THREAT	L	ML	M	MH	H
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M

INHERENT VULNERABILITY

Back to Table of Contents

Chapter 17: Dealers in Precious Metals and Stones

Summary Findings: The ML risk rating for the sector was MEDIUM, based on ratings of MEDIUM for inherent vulnerabilities and MEDIUM-LOW for ML threats. This finding remains the same as 2017 and is also attributed to the fact that Dealers in Precious Metals and Stones have low levels of cash associated with the transactions they conduct.

AML/ATF Supervisory Authority – Registrar of Companies

Introduction

The Dealers in Precious Metals and Stones (DPMS) sector in Bermuda is classified as jewelry dealers, and precious metals and stones dealers. The sector is very small and wholly composed of retail businesses. There are no wholesale importers or exporters in Bermuda and mining activities do not exist on-island. The sector contributed less than 1% to the gross domestic product of Bermuda during the relevant period:

- 2017 - $27.6 million
- 2018 - $13.6 million
- 2019 - $10.2 million

The level of cash activity, in particular large level transactions, within the sector is minimal. There are less than 30 retailers operating in this sector. Only 1 retailer offers loose stones for purchase on a regular basis. There is a low ratio of non-resident clients (seasonal transactions) versus annual purchases by residents. During the high tourist season (May-October) sales of jewelry increased due to Bermuda's tax-free status of many jewelry items.

AML/ATF supervisory oversight of DPMS transitioned from the Financial Intelligence Agency ("FIA") to the RoC with effect from 1 November 2020 pursuant to the Registrar of Companies (Supervision and Regulation) Act 2020 with consequential amendments made to the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 ("SEA") and associated AML/ATF legislative framework. The Regulations apply to this group if they intend to carry out cash transactions equal to or above B$7,500 or the equivalent in any other currency.

Assessment of Sectoral ML Threats

The DPMS sector was rated as MEDIUM-LOW for ML threats. There were no investigations or any intelligence about the sector being involved in ML during the review period. Nonetheless, it was also acknowledged that precious metals and stones are easily transportable and remain potentially attractive for moving criminal proceeds derived from drug trafficking. However, this threat is limited given the restricted size of cash transactions within this sector.

Back to Table of Contents

Analysis of Sector Inherent Vulnerabilities

The DPMS sector's inherent ML vulnerability rating remained as MEDIUM. This rating was driven by the minimal level of cash activity within the sector, in particular for large transactions. There also remained a low level of turnover/value of retailers in this group.

The sector contributed less than 1% to Bermuda's GDP during the review period with approximately $10.2 million generated in output.

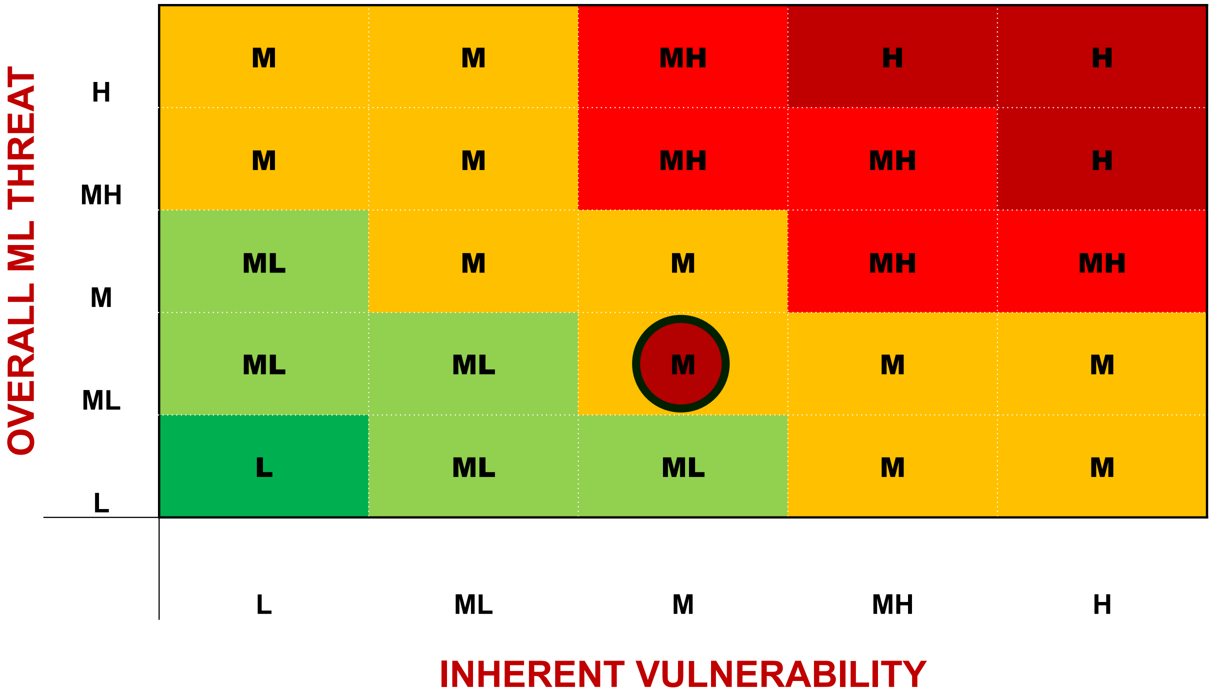
The sector's client base comprises all segments of Bermuda's community, including HNWIs. The ratio of domestic vs. international clientele was 70/30, primarily driven by seasonal tourism purchases. The sector has less exposure to corporate structures or legal entities, and any transactions with such clients are typically not cash-driven and do not involve foreign entities, therefore they are also highly traceable, along with beneficial ownership information. The DPMS sector has firm policies and procedures in place to not accept cash equal to or in excess of the BMD $7,500 statutory threshold.

There was little to no exposure for the sector to other vulnerability factors such as non-face-to-face transactions, fraud or tax evasion schemes and use of agents.

Conclusion

As shown in the heat map below, the inherent ML risk rating for the sector was MEDIUM, based on ratings of MEDIUM for inherent vulnerabilities and MEDIUM-LOW for ML threats. This finding remains the same as 2017.

Dealers in Precious Metals & Stones Inherent ML Risk Rating



OVERALL ML THREAT	L	ML	M	MH	H
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M

Back to Table of Contents

Chapter 18: Casino Gaming Sector

Summary of Findings: The ML risk rating of MEDIUM-LOW for the Casino Gaming sector remains as a conditionally offered score, since there are still no casinos operating in Bermuda. However, recognising that casino gaming can pose money laundering risks, this sector has been included in the National Risk Assessment proactively and based on international experiences in this area. The inherent vulnerability factors assessed are based on anticipated features of Bermuda's casino gaming industry. The inherent ML risk rating comprises an inherent vulnerability rating of MEDIUM and a ML threat rating of LOW.

AML/ATF Supervisory Authority – Bermuda Gaming Commission

Introduction

There were no casinos in operation during the review period.

For context, the Bermuda Gaming Commission (the Commission) is the established competent authority that will conduct regulation and supervision of casino gaming in Bermuda, based on five (5) key goals:

- That owners, vendors, managers, employees, and sources of finance should be free from any inappropriate past or present associations and behaviours, and should uphold high ethical standards;
- That operators should possess sound operational and financial controls;
- That the games offered should be fair, honest, and operate with a high level of security and integrity;
- That all fees, taxes, and related payments should be appropriately accounted for and paid; and
- That controls must be in place to protect the vulnerable, where operators conduct their business to protect consumers and the wider public from gambling related issues.

Bermuda is committed to implementing and maintaining a regime and approach that will protect its citizens and maintain public confidence by following principles of honesty, integrity, and social responsibility. Based on that commitment, the ultimate objective is to achieve effective regulation and a healthy culture of compliance within the industry.

Since the 2017 ML NRA, the regulatory framework for casino gaming was finalised. A comprehensive and internationally comparable set of supporting regulations for the Casino Gaming Act 2014 was enacted – the Casino Gaming Regulations 2018. No changes were made to the framework. The Commission is now responsible for licensing and regulating casino gaming, and supervising licensed casino operators for AML compliance.

The approval processes for casino operators and casino operations is rigorous, involving several stages. Assessments cover wide-ranging elements, from information in applications for designated site orders to in-depth reviews of the suitability (both financial and character) of applicants and their associates. Only upon successful completion of the suitability stage will a casino licence be granted.

Back to Table of Contents

Assessment of Sectoral ML Threats

Casino Gaming was rated LOW for ML threats, compared to medium in 2017, due to the continued absence of any gaming activity in this sector. However, it is acknowledged that globally money launderers target casino gaming, as it remains an attractive avenue for potentially laundering criminal proceeds at scale. The typologies are well known and Bermuda's authorities will continue to take them into account as the regulatory framework is built and matures.

Analysis of Sector Inherent Vulnerabilities

The inherent ML vulnerability rating for Bermuda's anticipated casino gaming sector was MEDIUM. More data was available for this assessment; highlights of the analysis focused on key vulnerability factors are shown below:

Client base

The prospective client base for the sector was rated as HIGH for ML vulnerability. This rating is based on the anticipated patrons of Bermuda's casinos having higher ML risk profiles, specifically:

- PEPs (both domestic and international)
- HNWIs (both domestic and international)
- Non-residents
- Foreign personal or business interests

It is likely that a substantial proportion of patrons will be from overseas, given that casinos in Bermuda must be part of a hotel/resort complex. However, there is no statutory bar to Bermudians or Bermuda residents being customers of casinos in the country. It is therefore very likely that domestic PEPs and HNWIs will form part of the casino's client base. It is also noted that, as the pool of persons visiting a resort is wide, persons with criminal records or past administrative and/or supervisory actions against them could be potential casino patrons.

Despite the expected international clientele, there is no evidence to suggest that Bermuda casinos will attract a large proportion of patrons from high-risk jurisdictions, or that existing visitor demographics - the vast majority of visitors to Bermuda are from the US East Coast and Canada - will change. Nonetheless, it cannot be ruled out that some patrons may originate from jurisdictions considered to be high-risk for ML.

Products and services

The inherent ML vulnerability rating for casino gaming products and services was MEDIUM-HIGH. Typical to the nature of casinos globally, the potential for misuse of products and services for ML purposes drove this rating. For example, casino chips, gaming equipment producing tickets for cash and player-to-player gaming all provide patrons with the equivalent of currency, which could potentially be transferred to third parties or removed from the casino and be difficult to trace. Other gaming facilities, such as tournaments, junkets and VIP rooms also present their own potential for misuse for money laundering.

Frequency of International transactions

This factor was assessed as having MEDIUM inherent ML vulnerability. Given that most patrons are likely to be non-resident, international transactions will be an inevitable aspect of the business model of casino operators. This will, however, take place within the context of the cashless gaming regulatory regime and systems under which Bermuda casinos must operate.

Use of agents

The use of agents in this sector was assessed as having MEDIUM inherent ML vulnerability. The use of agents, i.e. third parties introducing patrons

Back to Table of Contents

to a casino operator, is permitted and referred to as "casino marketing arrangements" under the relevant legislation. This reliance on third party introducers in the casino gaming sector globally is generally a known potential vulnerability to money laundering. Therefore the assessment took this into account, along with the fact that the applicants for Bermuda's pending casino licence applications are well known global casino operators who are likely to be approached by marketing agents. It was acknowledged that the extent of this vulnerability remains an unknown factor until a casino is actually in operation.

Other vulnerability factors assessed as posing a lower inherent vulnerability for ML in the prospective sector were:

Size of the sector

Relative to other sectors of Bermuda's economy, and based on the sector's comparative licensing and annual fees, the financial stature of the casino industry in Bermuda will be small to moderate.

Ability to trace financial transactions

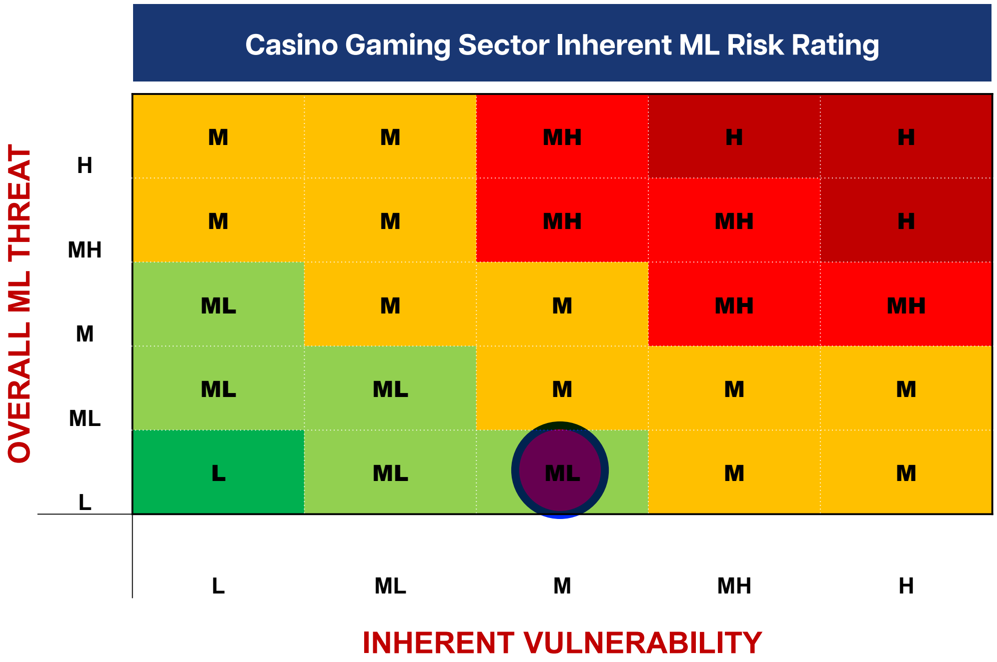
In light of the policy decision that gambling would be by way of cashless gaming, an operator will have to install a cashless wagering system. Given the prescribed requirements for such a system, it was determined that there will be little difficulty in tracing financial transactions.

Typologies and crimes featuring the sector

There are extensive typologies and examples of the casino gaming sector being used globally for ML and for tax and fraud schemes. The assessment showed that the key element making the industry attractive for ML schemes, and other criminal behaviour, was the high level of cash activity. As cashless gaming will apply in the Bermuda model, the rating for this vulnerability factor was determined to be low.

Conclusion

The ML risk rating of MEDIUM-LOW for the Casino Gaming sector remains as a conditionally offered score, since there are still no casinos operating in Bermuda. As shown in the heat map below, the inherent ML risk rating of MEDIUM-LOW comprises an inherent vulnerability rating of MEDIUM and a ML threat rating of LOW.



Casino Gaming Sector Inherent ML Risk Rating

OVERALL ML THREAT					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

INHERENT VULNERABILITY

Back to Table of Contents

Chapter 19: The Betting Sector

Summary of Findings: The ML risk rating for the Betting sector is MEDIUM. This rating comprises a medium rating for both inherent vulnerabilities and ML threats for the sector. The sector's small size in Bermuda, coupled with the small size of transactions, lessens its attractiveness for money laundering. However, the assessment takes into account the typically widespread use of cash in the sector, and possible existence of PEPs or other high-risk clients among its client base.

AML/ATF Supervisory Authority – Bermuda Gaming Commission

Introduction

The Betting sector in Bermuda is relatively small and currently comprises three operators with five locations. During the review period (Jan 2017 to Dec 2019), the sector was subject to a licensing regime under the Betting Act 1975 and licensees are subject to betting duties imposed under Bermuda's Taxes Management Act 1976 and associated Regulations. This legislation has since been repealed and replaced with the Betting Act 2021, which came into force in August 2021. Betting duty collected over the course of the review period had declined steadily and significantly. Although the sector was subject to licensing under the 1975 Act, the Bermuda Betting Licensing Authority did not have traditional regulatory powers, nor was it operational full time, thus there was no active supervision nor oversight of the operations within the sector.

Only individuals could place bets through local licensed betting establishments. Companies and legal entities or structures are restricted from betting. The betting industry offered the following products:

- International sports betting
- Live bingo
- Online casino-type gaming (slot machines and spinners)

The relatively small size of the industry has facilitated the development of self-imposed AML controls within each establishment. Placement of bets by the wide majority of patrons occurs in person. The country is small and this sector is small. Therefore, management and staff of licenced establishments have been able, over the course of the review period, to gain personal knowledge and insight into their patrons. All bets are recorded. In some very limited circumstances, customers are able to open deposit accounts with the licensee; they can then, in person, submit cash on the account which they may use to place bets. In even more limited cases, some of these customers lodge a credit or debit card with the licensee and then approve small amounts to be debited from these cards over the phone with staff who are clear about their identity. Winnings are deposited onto customer deposit accounts but are not credited to credit or debit cards. Winnings can also be claimed in cash at very low amounts per day ($1,500). There are no transfers of funds of any type to or from customer's bank accounts.

Back to Table of Contents

Assessment of Sectoral ML Threats

The ML threat rating of Medium for this sector was again justified, compared with the 2017 medium rating. Only one (1) ML investigation was associated with this sector during the 2020 review period, and there continued to be no reporting of suspicious activities from this sector. Law enforcement intelligence suggests that the sector is still able to be misused by gang members whose main source of income is drug trafficking. The sector is primarily cash-based and at present the client account facility offered in some operations seem to have featured in the known cases. During the review period, drug trafficking was rated as a High ML threat for Bermuda, and this was factored in, when assessing this sector. However, the small size of the sector was also balanced against this, as the amount of funds that flow through the sector is germane to the scale of ML that can be accommodated through the sector at any given time.

Analysis of Sector Inherent Vulnerabilities

The Betting sector's inherent vulnerability to money laundering was rated as MEDIUM. The factors examined in the assessment included all the inherent features of the sector, such as size of business, clientele, product offerings, and payment mechanisms, among others.

Most of the inherent vulnerability factors were assessed as having LOW vulnerability. This was primarily due to the small turnover of the sector[31]; the absence of the use of agents; the fact that there is no capacity for anonymous use of the products and services offered; that globally this sector is not known to feature in tax evasion and/or fraud schemes; transactions are easily traced; and the limited availability of non-face-to-face transactions.

Some vulnerabilities were identified:

- the inability to definitively rule out the existence of some higher risk clients in the sector
- the predominant use of cash
- the fact that globally the sector features in some international ML typologies, albeit not in recent circumstances

Typologies also indicate that betting not consistent with patron profiles, frequent betting in amounts just less than fixed thresholds and buying winnings offering cash at a premium from legitimate customers are ways in which the sector can be used for money laundering.

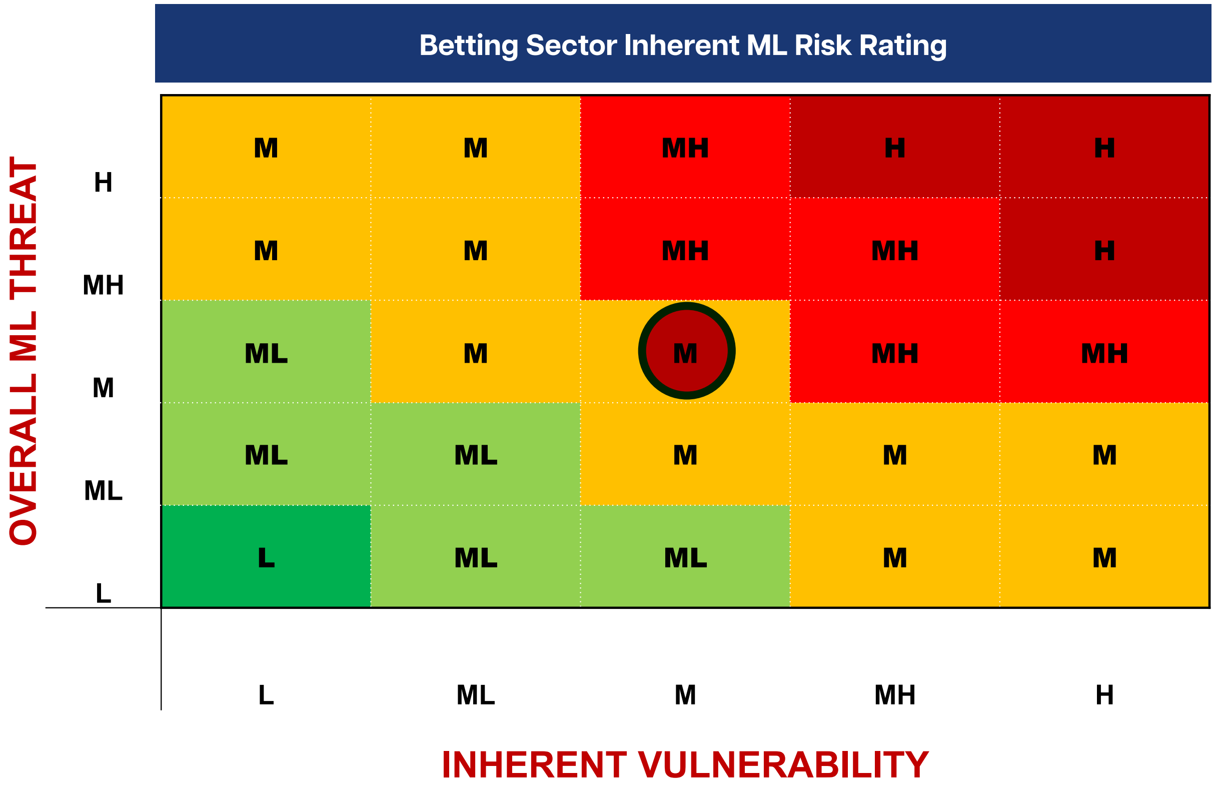
It was established that betting in this sector is cash-intensive, and also that some patrons may be PEPs, have criminal records or may have business or personal ties to foreign jurisdictions. Nevertheless, the self-imposed deposit, betting and winning limits by the licensees, together with the resulting small transaction amounts, reduces the potential for even moderate sums of money to be laundered. Typically, across the sector, bets averaged between twenty to a few hundred dollars. The international typologies that feature the betting sector are few and far between. But, over the course of the review period, domestic law enforcement agencies indicated that whenever suspected criminals justify the origins of suspected proceeds of crime by asserting they are the winnings of betting within this sector, it is not always easy to determine the funds were legitimately disbursed by a licensee in this sector. The absence of record keeping obligations on the sector allows for betting firms to keep different levels of disbursement details.

[31] Betting duty was used as the only available metric for this assessment, as it is levied as a percentage of amounts wagered. Available information indicates that betting duty collected over the course of the review period represents less than 0.2% of the Government's total revenue.

Back to Table of Contents

Conclusion

As shown in the heat map below, the ML risk rating for the Betting sector is MEDIUM. This rating comprises a MEDIUM rating for both inherent vulnerabilities and ML threats for the sector.



Betting Sector Inherent ML Risk Rating

OVERALL ML THREAT					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

INHERENT VULNERABILITY

Back to Table of Contents

Chapter 20: Dealers in High-Value Goods

Summary Findings: The ML risk rating for the sector remained MEDIUM-LOW. This rating comprises a MEDIUM-LOW rating for inherent vulnerabilities and a LOW ML threat rating for the sector. This finding is also attributed to the fact that the level of cash activity within the sector, in particular large level transactions, was minimal. There also remained a low level of turnover/ value of retailers in this group, and a low risk client base.

AML/ATF Supervisory Authority – Registrar of Companies

Introduction

The Dealers in High Value Goods sector (HVD/ DiHVG) in Bermuda is classified as car, boat and motorcycle dealers, antique dealers and auctioneers. The sector is wholly composed of retail businesses and there are no known wholesale importers or exporters in Bermuda. The sector contributed less than 1% to Bermuda GDP during the review period:

- 2017 - $24.5 million
- 2018 - $24.1 million
- 2019 - $21.4. million

The level of cash activity, in particular large level transactions, within the sector is minimal. There are less than 30 retailers operating in the sector. There is a low ratio of non-resident clients due to residency restrictions on purchasing cars, and licensing requirements for the operating boats within the jurisdiction. Businesses may purchase vehicles, however these can only be used for commercial purposes and the number of vehicles that can be licensed and operated for commercial purposes is strictly monitored by the Transport Control Department.

AML/ATF supervisory oversight of DiHVGs transitioned from the Financial Intelligence Agency ("FIA") to the Registrar of Companies (RoC) with effect from 1 November 2020 pursuant to the Registrar of Companies (Supervision and Regulation) Act 2020, with consequential amendments made to the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 ("SEA") and associated AML/ATF legislative framework. The Regulations apply to this group if they intend to carry out cash transactions equal to or above BMD $7,500 or the equivalent in any other currency.

Assessment of Sectoral ML Threats

The ML threat rating for the sector remains LOW. There was no evidence that the institutions' products in this sector were used or could be used successfully for money laundering.

Back to Table of Contents

Analysis of Sector Inherent Vulnerabilities

The HVD sector's inherent vulnerability rating remained MEDIUM-LOW, as in 2017. This rating was driven by the minimal level of cash activity within the sector, in particular for large transactions. There also remained a low level of turnover/ value of retailers in this group, and a low risk client base.

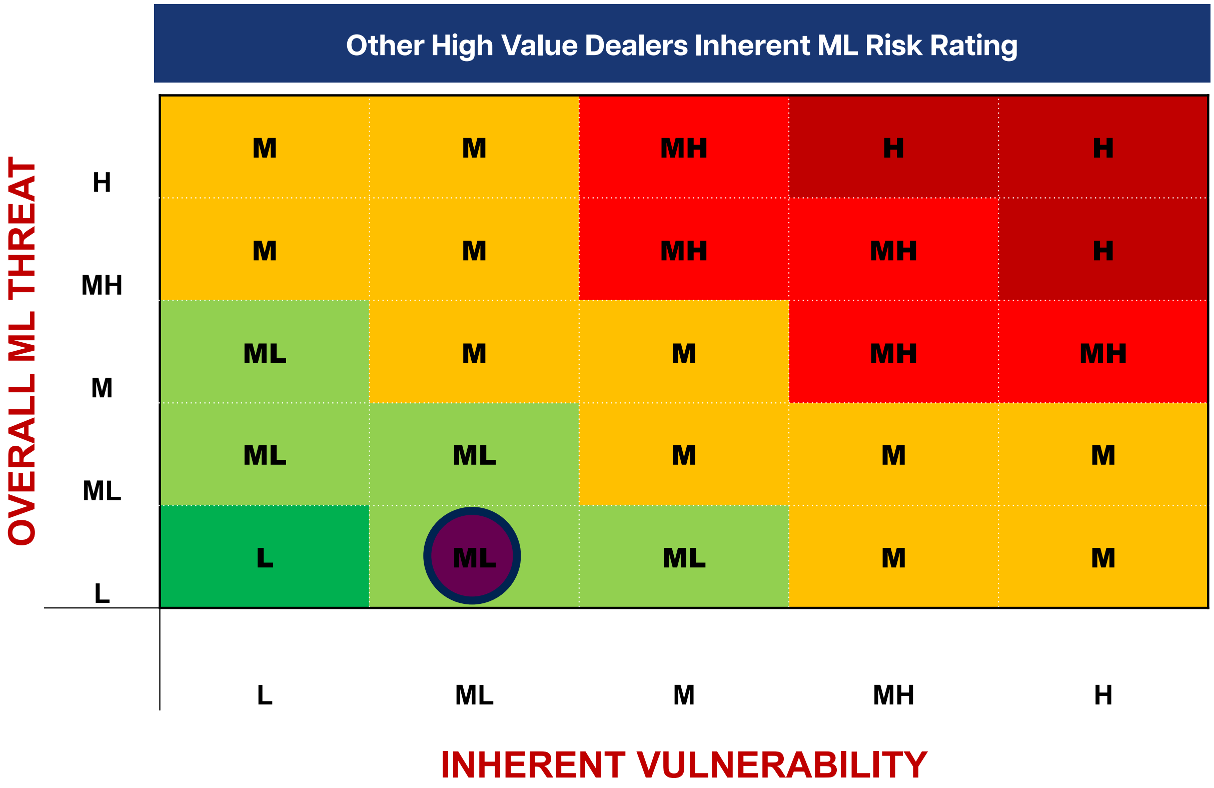
The total contribution (all sales) of the HVD sector to Bermuda's GDP for each year during the reporting period was less than 1% of GDP. As at 31 December 2019 the contribution to GDP was $21.4 million or 0.30% of GDP.

The clientele of the HVDs sector were predominantly individuals. Clients could include HNWIs and PEPs, however given the high level of non-cash transactions for purchases and the licensing and/ or registration requirements related to buying cars, boats and other products offered in the sector, transactions can be easily traced. The sector has less exposure to corporate structures or legal entities, and any transactions with such clients are typically not cash-driven and do not involve foreign entities, therefore they are also highly traceable, along with beneficial ownership information. HVDs have firm policies and procedures in place to not accept cash equal to or in excess of the BMD $7,500 statutory threshold.

There was no exposure for the sector to other vulnerability factors such as non-face-to-face transactions, fraud or tax evasion schemes and use of agents.

Conclusion

As shown in the heat map below, the inherent ML risk rating for the sector remained MEDIUM-LOW. This rating comprises a MEDIUM-LOW rating for inherent vulnerabilities and a LOW ML threat rating for the sector.



Other High Value Dealers Inherent ML Risk Rating

OVERALL ML THREAT	L	ML	M	MH	H
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M

ASSESSMENT OF TF RISKS

Chapter 21: Terrorist Financing National Risk Assessment

Introduction

Bermuda's comprehensive ATF legislative and supervisory frameworks, with ongoing enhancements and updates, has supported the Bermuda Government's long-standing and continued commitment to combatting terrorism and terrorist financing, domestically and globally:

- **Core Legislation** - Enacted in 2004, the Anti-Terrorism (Financial and Other Measures) Act, is the primary legislation criminalising fundraising for the purpose of terrorist financing.

- **Targeted Financial Sanctions** - Bermuda also implements, in cooperation with UK authorities, targeted financial sanctions as required by the United Nations Security Council, as well as sanctions imposed by the UK, through UK legislation extended to Overseas Territories by sanctions-related Orders in Council.

- **Strong Inter-Agency Coordination** - Five agencies in Bermuda cooperate closely on TF-related intelligence, enforcement, prosecutions and asset recovery: the Financial Intelligence Agency (FIA), the Bermuda Police Service, the Department of Public Prosecutions, the Customs Department and the Attorney-General's Chambers.

- **Effective Regulatory Framework** - Those agencies also collaborate with relevant supervisory bodies in Bermuda. These bodies have extensive regulatory and supervisory toolkits to ensure they can effectively monitor and enforce compliance with ATF provisions within Bermuda's legislative framework. During the review period for this NRA, the relevant supervisors were: the BMA, for regulated financial institutions; the Financial Intelligence Agency[32]; the Superintendent for Real Estate; the Barristers and Accountants AML/ATF Board for lawyers and accountants in independent practice; and the Registry General, which oversees charities.

- **International Cooperation** - Bermuda's commitment to the global fight against terrorism financing includes providing assistance to foreign countries for criminal investigations in this context. The Attorney-General

[32] The FIA has since transferred this supervisory function to the Registrar of Companies by virtue of legislative amendments made to SEA, and the enactment of the Registrar of Companies (Supervision and Regulation) Act 2020, which came into force on 1 November 2020.

Back to Table of Contents

is the Central Authority for mutual legal assistance requests related to TF offences and criminal proceedings or investigations that have begun in other countries. Other agencies, including the FIA as a member of the Egmont Group, also actively participate in Bermuda's international cooperation activities.

The 2020 Terrorism Financing National Risk Assessment ("2020 TF NRA") recognises this collective commitment to maintaining a robust ATF regime, while determining the overall risk of terrorist financing in Bermuda. This assessment will support any work to update the framework further if necessary as changes in the global market and international requirements emerge.

The 2020 Assessment

The 2020 TF NRA built upon the 2016 assessment, with updates reflecting any notable changes globally to the terrorism landscape, and consideration of new factors not previously evaluated. Underpinning the assessment, as before, was the FATF's definition of a "terrorist act", and "terrorist financing". A terrorist act includes offences under a range of widely adopted international conventions and treaties. FATF's related definition of "terrorist financing" is therefore any financing of terrorist acts, and of terrorists and terrorist organisations. This can include providing funds from criminal activity and also funding from legitimate origins.

Within Bermuda's ATF regime, the meaning of "terrorism" is provided in section 3 of the Anti-Terrorism (Financial and Other Measures) Act 2004, and aligns with the FATF's definition of "terrorist act". The underlying cause of an act is what determines if it is to be considered an act of terrorism. There is a distinction between actions driven by criminal motives of greed and passion as opposed to actions driven by ideology or cause, the latter of which gives rise to terrorism.

In preparation for the 2020 TF NRA, Bermuda's law enforcement, financial intelligence and national security intelligence agencies, reviewed the current scope of terrorism potentially affecting Bermuda. During the planning stage of the NRA, it was acknowledged that Bermuda had not experienced any terrorism and that there was no evidence of planning for terrorism during the assessment period.

As with the 2016 NRA, the agencies reviewed the global terrorism landscape, including significant terrorist organisations and their operations, to compile a list of terrorist organisations that could potentially present a threat to Bermuda. Factors considered included the expansion or merger of existing terrorist organisations, as well as the potential impact of international counter-terrorism efforts on the efficacy of these organisations. The previous list of terrorist organisations from the 2016 TF NRA was updated on that basis for this assessment.

Back to Table of Contents

The terrorist organisations were also selected based on their potential connection to Bermuda, and how such connections could pose a threat to the country. Key factors in that analysis included funding sources and operational scope of the terrorist organisations; whether there were diaspora groups in Bermuda from the countries in which these organisations primarily operate or have influence; and related immigration patterns and foreign-based demographics. Economic and political factors were also taken into account, such as the direction and sources of international business, as well as Bermuda's economic and political ties to major trading partners such as the UK, US and the EU.

Methodology and Scope

A single working group comprising representatives from NAMLC and Bermuda's judicial, prosecutorial, law enforcement, financial intelligence, asset recovery, immigration, border control and supervisory agencies conducted the 2020 TF NRA. The working group also sought input from the private sector, via consultation with representatives from Bermuda's financial services sector, as well as the legal, accounting and non-profit sectors.

As was done in 2016, the 2020 TF NRA was based on the World Bank's TF Risk Assessment Module, which relies on quantitative and qualitative data to evaluate the threat of terrorism in a country; and the threat of terrorist financing occurring in, from, to or through that country. The methodology for the assessment comprises three main components:

i. **Terrorism Threats** – this assessment examined the sources of domestic, regional and global threats of terrorist activity potentially targeting Bermuda. It also evaluated the threat of Bermuda being used for terrorist activity conducted in other countries.

ii. **Terrorist Financing Threats** – this assessment examined the direction, sources and channels of funds which could potentially feature in terrorism financing activities in Bermuda, should the country be targeted for this purpose; and

iii. **Terrorist Financing Vulnerability** – this assessment involved identifying and assessing the adequacy of the key controls required to deter, detect and counter-terrorist financing in Bermuda.

However, in this report, only the findings related to inherent risk, namely the outcomes of the Terrorism Threat and TF Threat assessments are provided. However, the TF Vulnerability assessment in the 2020 TF NRA has confirmed the effectiveness of Bermuda's risk-based ATF framework, as reflected in Bermuda's 2020 Mutual Evaluation Report.[33]

[33] Published on the FATF's website: https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/CFATF-Mutual-Evaluation-Report-Bermuda-2020.pdf

Back to Table of Contents

As part of the terrorism threat assessment, the analysis of terrorist organisations used work previously conducted in this regard during Bermuda's 2016 TF NRA, supplemented with updated source material. These sources included but were not limited to:

- 2016 United Kingdom's Proscription of Terrorist Organisations (reviewed by the UK Home Office);
- United States Terrorist Exclusion List and Foreign Terrorist Organisation List (reviewed by the US State Department);
- United Nations Office on Drugs and Crime;
- United Nations Security Council Resolutions (UNSCR) 1267 and 1373 and their successor resolutions; and
- Stanford Centre for International Security and Cooperation.

As an Overseas Territory of the UK, significant reliance was placed on UK sources and assessments, as it is likely that Bermuda's exposure to terrorism threats might also be affected by threats to the UK. The 5-point rating scale used in the Terrorism Threats assessment is based on the UK's MI-5 Threat Level Scale. The UK's threat levels are designed to give a broad indication of the likelihood of a terrorist attack, namely:

- Low means an attack is highly unlikely – this aligned with the NRA rating of Low
- Moderate means an attack is possible, but not likely – this aligned with the NRA rating of Medium-Low
- Substantial means an attack is likely – this aligned with the NRA rating of Medium
- Severe means an attack is highly likely – this aligned with the NRA rating of Medium-High
- Critical means an attack is highly likely in the near future – this aligned with the NRA rating of High

Back to Table of Contents

Chapter 22: Terrorism Threat

The working group's first phase of analysis for the 2020 TF NRA covered key factors that would contribute to terrorist threats to or from within Bermuda, as well as the threat of terrorist financing being conducted in or through the jurisdiction. The overall assessment findings in each of those areas are shown below.

Methodology and Scope

The assessment of terrorism threat involved the examination of the sources of domestic, regional and global threats of terrorist activity potentially targeting Bermuda and also included consideration of the threat of Bermuda playing a role in terrorist activity in other countries. A significant component of such an assessment would usually rely on examining cases and evidence of terrorism in the country or region. Thus all intelligence and law enforcement sources were also examined to identify if there is any evidence of terrorism in the country also.

Evidence of Terrorism

The four factors listed in the table below were considered in determining the level of physical terrorism threat to Bermuda, either from terrorist organisations or individuals. The analysis reviewed the period between January 2017 and December 2019, and concluded that there is no evidence of terrorism originating in Bermuda or targeting other countries from within Bermuda.

Table 5: Physical Terrorism Threat Factor

Physical Terrorism Threat Factor	Reported Activity: 2017 - 2019
Property damage	Bermuda experienced no property damage that law enforcement attributed to acts of terrorism
Casualties	Bermuda did not experience any casualty (either injury or death) that law enforcement attributed to acts of terrorism
Cases investigated, prosecuted and convicted	Bermuda law enforcement did not criminally investigate any domestic terrorist cases or receive any international requests for assistance relating to terrorism activity in the jurisdiction, prosecute any terrorism cases or record any terrorism-related criminal convictions
Nature of international cooperation undertaken or provided	Bermuda law enforcement engaged and responded to international law enforcement agencies (LEA) and national security intelligence partners' requests, but none of these requests resulted in terrorists' targets or activities being identified in Bermuda, as the nature of the requests was to provide information only to support other countries' ongoing investigations.

Back to Table of Contents

Origin/Sources of Terrorism Threats

The assessment of the origin and sources of terrorism is based on evaluating four terrorism threat components: Domestic Threats, Regional Threats, Global Threats and Use of Bermuda as a Transit Point. The analysis determined that there is no domestic terrorist organisation known to be operating from within Bermuda, and no international or regional terrorist organisations, foreign terrorist fighters or self-radicalised terrorists known to be targeting Bermuda.

This is consistent with the findings in the 2016 NRA, and any changes in the global or regional landscape have not adversely affected Bermuda's exposure to terrorism threats. Table 1 summarises the overall 2020 NRA ratings for each broad component of terrorism threats, followed below by more detailed analysis and findings on related sub-elements.

Table 6: Overall Ratings for Terrorism Threat Components 2016 vs 2020

Terrorism Threat Component	Description	2016 Ratings	2020 Ratings
Domestic Threats	Originating within Bermuda and targeting Bermuda	Medium-low	Low
Regional Threats	Originating from within or outside the region, and targeting the region including Bermuda	Not rated	Low
Global Threats	Originating from any source within the globe and targeting Bermuda, or originating in Bermuda and targeting anywhere within the globe	Low	Low
Bermuda as a Transit Point	Use of Bermuda as a staging or transition location for terrorist cells or organisations from another country and targeting a third country	Not rated	Low

Regarding Domestic Terrorism, the analysis mainly focused on whether or not there are radicalised persons within Bermuda, particularly in two categories: Lone Wolf Actors or Foreign Terrorist Fighters (FTFs). The assessment confirmed that there is no known evidence of radicalisation within the resident population. It also found that: a) no Lone Wolf Actors or FTFs carried out terrorism acts in Bermuda for the reporting period; and b) there have been no cases of Bermuda residents operating as, or travelling to become, FTFs in other parts of the world and therefore that Bermuda faces no real threat from returning FTFs. The rating was therefore assessed as **Low.**

Regional terrorist threats were assessed for the first time. For the purposes of this assessment the "region" encompassed Bermuda, the Americas (North, Central and South) and the Caribbean. The potential sources of regional threat to Bermuda were considered to be: a) an act of terrorism in Bermuda

Back to Table of Contents

by someone from within the region; or b) an act of terrorism in Bermuda as part of an attack on the region. Having considered international sources of information as well as intelligence from local law enforcement and financial intelligence agencies, it was determined that there are no identified active terrorist organisations in the region. There was no intelligence indicating that, from a regional perspective, Bermuda is likely to be subject to an attack. Bermuda's geographic isolation, economic and social dynamics, strong immigration policies and scrutiny in respect of foreign guest workers and expatriate residents, and lack of foreign military installations are also mitigating factors when assessing regional terrorism threats. All of these factors resulted in the rating of **Low.**

With respect to Global Threats, also rating as **Low**, examining the previously mentioned selected list of terrorist organisations with potential relevance to Bermuda was core to this part of the threat assessment. The assessment also included reviewing applicable data, as well as the scale of likely support and/or sympathizers from various diaspora groups in the resident population and the global outreach of each terrorist organisation (including any possibility for them to target or operate in Bermuda). The table below shows the threat ratings assigned to each terrorist organisation for both the 2016 and 2020 assessments. Based on shifts, mergers and dissolutions among the terrorist organisations themselves, nine of the terrorist organisations considered in 2016 remained on the 2020 list and 3 new organisations/groups of organisations were added:

Table 7: Threat Rating for Global Terrorist Actors (2020 vs 2016)

Global Terrorist Actors	2016 Threat Rating	2020 Threat Rating
a. Islamic State of Iraq and Syria (ISIS)	Low	Low
b. Al Qaeda (AQ) aka al-Qaida / al-Qa'ida	Low	Low
c. Abu Sayyaf (Philippines)	Low	Low
d. Al Shabaab	Low	Low
e. Hamas	Low	Low
f. Haqqani Network	Low	Low
g. Hezbollah (Military Wing)	Low	Low
h. Jabhat Al-Nusra is now Hay'at Tahrir al-Sham	Low	Low
i. Turkmenistan Islamic Party aka ETIP, ETIM and HAAT [34]	Medium-Low	Medium-Low
j. Irish Terrorist Organizations[35]	Not Rated	Low
k. Mujahideen Indonesia Timur	Not Rated	Low
l. Lashkar y Taiba LT (aka Lashkar-e-Taiba / Lashkar-i-Tayyeba)	Not Rated	Low
m. Foreign Terrorist Fighters (locals going abroad as FTFs)	Not Rated	Low
n. Foreign Terrorist Fighters (foreigners coming to Bermuda as FTFs)	Not Rated	Low

[34] This was based on the fact that this organisation is operated by Uighur militants in western China and there is the continued presence of a tiny ethnic diaspora population in Bermuda. This latter fact was balanced by the absence of any actual local or foreign-sourced intelligence to suggest affiliation with or influence by this organisation within this diaspora group and thus justified this threat rating in 2020.

[35] An amalgam of fourteen separate organisations, representing nationalist and unionist ideology respectively, broken down into two broad groups namely: i) Nationalist/Republican/Catholic group (6 organisations); and ii) Unionist/Loyalist/Protestant group (8 organisations).

Back to Table of Contents

There was no indication that Bermuda is being used by these terrorist organisations or related FTFs. However, several other related factors were also assessed, including terrorist organisations or individuals conducting terrorist acts during major events generating international attention or media coverage, or during visits by high-profile global figures. Bermuda's continued vigilance in this context, despite the predominantly low threat ratings, will include ongoing monitoring of terrorism trends relevant to these groups and contexts globally.

The threat of Bermuda being used as a transit point for terrorist activity was also assessed for the first time. Several factors indicated that Bermuda is not an attractive jurisdiction for supplying logistical and/or strategic support for terrorist activity, resulting in a threat rating of **Low**. These factors include Bermuda's isolated geographic location, lack of proximity to current war zones, stringent immigration procedures and evidence or intelligence from law enforcement agencies.

Impact on Terrorist Financing

The assessment of terrorism threats also considered their potential impact on terrorism financing. This included assessing funding sources of the selected terrorist organisations, and considering links to Bermuda's local population and foreign resident groups. The purpose of this was to determine which terrorist actors presented a greater potential of exploiting Bermuda's financial mechanisms in order to fund their activities.

When all twelve international terrorist organisations on the 2020 list were examined, all but four were rated as having a low potential impact on TF in Bermuda, while FTFs were also rated low in this regard. This was because they either did not use global funding sources, or they had non-existent or insufficient potential for connections with Bermuda, e.g., no or low level of diaspora populations in Bermuda who could be targeted for funding. Four of the twelve terrorist organisations were rated as having a potential Medium-Low impact on TF, as there was some evidence that they solicit funds from global sources, including from diaspora populations around the world. This factor had to be considered in light of the presence of various relevant diaspora groups in Bermuda, even though there is no actual evidence of funding support or any actual cases of TF originating from Bermuda.

Conclusion

In light of the findings that the domestic, regional and global threats of terrorism to Bermuda were all assessed as low, as well as the rating of low for the threat of Bermuda being used as a transit point for terrorism, it was determined that **Bermuda's overall Terrorism Threat rating was LOW.** This is the same as in 2016, with largely similar reasons for this rating. Bermuda's unique circumstances relating to economic, social, geographical and demographic factors all work together to mitigate the potential terrorism threats to Bermuda.

Back to Table of Contents

Bermuda authorities are not complacent about this finding and are mindful of the fact that this is not an indication that terrorism could never occur in Bermuda, nor that persons in Bermuda could never try to engage in terrorist activity here or abroad. Therefore authorities will continue to remain vigilant, take steps to share any terrorism-related intelligence and to work cooperatively to keep the threat of terrorism at bay.

Regarding the impact of the Terrorism Threat findings on Terrorism Financing in Bermuda, the analysis shows that although the impact is at the lower level, private sector stakeholders must maintain vigilance around the transactions and activities of persons and entities that interact with higher risk countries, especially those in which there are active terrorist organisations that source their funding globally.

Back to Table of Contents

Chapter 23: Terrorism Financing Threats

Introduction

The 2020 TF threat assessment updated 2016's findings while also relying on the conclusions of this NRA regarding terrorism threats to Bermuda. The 2016 NRA assessed that the overall TF threat in Bermuda was Low and the 2020 MER confirmed the credibility of this finding. A similar approach to that used in 2016 was again applied to this assessment.

As there have been no confirmed cases of TF in Bermuda, nor any international TF cases with a Bermuda connection, Bermuda proactively used international TF typologies as an additional analytical tool to support this assessment of TF Threats. The typologies helped to analyse potential directions, sources and channels of funds, namely, how and whether Bermuda's economic sectors might be exposed to TF, based on funding methods and techniques seen in relevant scenarios within each typology.

The analysis determined that an overall rating of LOW for Terrorist Financing Threats to Bermuda was appropriate. This is the same as in 2016. While there is no evidence for Bermuda being a source of TF, the jurisdiction has made a number of recommendations to strengthen its ATF framework to ensure that the regime remains robust and is able to adapt appropriately to any emerging TF threats.

Methodology and Scope

The World Bank's assessment framework was used to determine Bermuda's TF threat profile. The WB methodology provides a systematic mechanism to assess and understand TF threats, but relies heavily on statistics and qualitative data about real cases. Since limited data was available in Bermuda given the lack of TF cases, as with the 2016 assessment, the decision was made to supplement the methodology by using selected international TF typologies.

The typologies helped determine the potential for known TF methods and techniques to occur in Bermuda, by examining all components of the national ATF framework. This analysis assisted primarily with assessing the sectoral channels in Bermuda that could potentially be targeted for TF activities.

The assessment of TF threats involve the assessment of 3 components, namely the:

- Direction of funds;
- Sources of funds; and
- Channels of funds.

Direction of Funds

An analysis of the cases to determine the intended destination of the funds in each case, which is largely dependent on the location of the terrorist activity or operation being supported.

TF cases and guidance from the FATF have shown that for all jurisdictions the funding to support terrorist activity, terrorists or terrorist organisations flows in the following potential directions:

Back to Table of Contents

i. Funds generated in the home jurisdiction for operations within the home jurisdiction;

ii. Funds generated in the home jurisdiction for operations within a foreign jurisdiction;

iii. Funds generated in a foreign jurisdiction for operations within the home jurisdiction

iv. Funds generated in a foreign jurisdiction for operations in other foreign jurisdictions (transit point); and

v. Origin and destination of funds cannot be identified.

These categories were used for the purpose of this analysis, together with any relevant findings from the Terrorism Threat assessment and any domestic or relevant foreign-based TF cases/investigations or reports/intelligence; the conclusions are summarised below:

I. Funds generated in Bermuda for operations within Bermuda – Rating LOW

As indicated in the terrorism threat assessment, there is no evidence of terrorist organisations or individual terrorists operating in Bermuda, and no terrorism activity has occurred in the jurisdiction. There is no actual intelligence or evidence to suggest that terrorism funding activity takes place in Bermuda. Therefore, the threat of domestic funding to support domestic terrorism was assessed to be low. The rating remained the same as in 2016, which was based on reasons similar to those highlighted above.

II. Funds generated in Bermuda for operations within a foreign jurisdiction – Rating LOW

This rating also remained the same as 2016, based on the following findings in 2020:

- As determined in the terrorism threat assessment, there was no evidence of Bermudians having been radicalised, such that they would fund and be supportive of overseas terrorist activity.

Back to Table of Contents

- Neither the BPS, FIA nor the BMA has had any intelligence or evidence to suggest that terrorism funding activity has taken place in Bermuda.

- Furthermore, Bermuda's 2020 Mutual Evaluation Report (MER) confirms that Bermuda has a good understanding of its TF risk profile,[36] and that the authorities have conducted effective TF investigations involving suspected TF related to the transfer of funds from Bermuda to high risk countries.[37] Although the investigations ultimately confirmed that there was no terrorism financing involved, the reason for the suspicion and resulting investigation was that funds were being remitted to a country that the reporting entity considered to be higher-risk for terrorism.[38] These investigations, therefore, highlight that financial institutions are aware of such matters, have appropriate controls for detection and are filing SARs in that regard.

- There is also a low likelihood that TF is taking place in Bermuda but remains undetected. Neither the FIA or BPS had received any intelligence or requests for assistance from foreign counterparts indicating that Bermuda has played any role in the funding of terrorist activity in other countries. Similarly, the Attorney-General's Chambers has received no Mutual Legal Assistance requests relating to foreign terrorism financing or foreign terrorism investigations.

III. Funds generated in a foreign jurisdiction for operations within Bermuda – Rating LOW

Consistent with the previous assessments relating to direction of funds, there is no intelligence nor evidence to suggest that terrorism funding activity takes place outside of Bermuda to support activities in Bermuda. As there is no evidence of domestic terrorism activity, it is highly unlikely that foreign sources of financing would be undertaken to support terrorism in Bermuda. The rating therefore remains at Low.

[36] See Chapter 2 (paras. 104 – 124), Bermuda's Mutual Evaluation Report, January 2020

[37] See Chapter 4, Bermuda's Mutual Evaluation Report, January 2020

[38] The country in question was also included on the list of higher risk jurisdictions, which the WG developed as part of the assessment.

Back to Table of Contents

IV. Funds generated in a foreign jurisdiction for operations within other foreign jurisdictions (transit point) – Rating LOW

The rating is low for this category as there are no cases that have occurred nor any intelligence to suggest that Bermuda is being used as a transit point in this way. There have been no domestic or foreign investigations nor any domestic or foreign-sourced intelligence to provide evidence that Bermuda is being, or has been, used as a transit point for the movement of terrorist funds from one country to another. A broad spectrum of international TF typologies was considered, and having examined them in the context of Bermuda's financial and DNFBP sectors it was determined that there are no special features, products or other factors that would make Bermuda uniquely targeted for this purpose.

V. Origin and destination of funds cannot be identified – Not Rated

In the absence of any actual cases or investigation that would fit in this category, it was determined that it was not appropriate to attempt to rate this category. This element can only be assessed based on real cases, thus the typologies were not useful in this regard.

Sources of Funds

In assessing the potential Sources of Funds that could be used for TF in Bermuda, all legitimate and illegitimate sources were considered, with particular focus on the following:

I. Charitable funds from Non-profit Organisations (NPO) - **Rating - LOW**

There is no evidence that non-profit organisations in Bermuda have been used for TF. Bermuda has a strong and robust framework for supervision of NPOs and has done considerable work to understand the nature and scope of activities such entities conduct. Further, 90% of Bermuda's registered NPOs only provide funding and charitable services to the domestic market. The majority of the remaining 10% of registered NPOs who provide funding for foreign charitable activities are engaging with jurisdictions that are low risk for terrorism. Only one NPO engages with a higher risk jurisdiction, and it is subject to close review by its supervisor.

Bermuda also allows privately funded charities, who are serviced by a licensed trust or corporate service provider, to be exempt from registration.

Back to Table of Contents

These exempted charities are generally sophisticated entities with appropriate systems and controls to allow for close scrutiny of beneficial ownership and how their funds are used, they do not solicit funds from the public and are likely to fund charitable activities outside of Bermuda. Since the majority of privately funded charities are managed and/or administered by a licensed TSP, therefore their charitable activities are subject to a high degree of control for both prudential and AML/ATF purposes.

II. Legitimate corporate income/profits or legitimate personal income/wealth - **Rating - LOW**

There is also no evidence that legitimate corporate income/profits or legitimate personal income/wealth have been used for TF. As highlighted previously, vigilance and a SAR submission from one financial institution led the BPS to investigate one case that involved the transmission to a high-risk jurisdiction of legitimately earned personal income. However, after local investigation, supported by foreign counterparts, it was confirmed that this transaction was not terrorist financing and was indeed legitimate. There have been no other cases nor intelligence, whether sourced domestically or from international counterparts, to suggest any other such transactions have taken place.

III. Proceeds from Criminal activity (including donor funds) - **Rating - LOW**

There have also been no cases, investigations or intelligence (domestic, international or foreign-sourced) to suggest that criminal proceeds derived from criminal activity in Bermuda have been directed towards terrorism anywhere else in the world.

In light of the conclusions and analysis above, it was determined that the rating of Low for all 3 potential sources of funds, is appropriate.

Channels of Funds

In the absence of confirmed TF cases, the TF Typologies[39] were analysed in detail to see the methods and techniques used in other jurisdictions to move terrorism funding. The analysis determined whether these methods could be duplicated, and how easy or difficult it would be to do so in Bermuda. All sectors subject to AML/ATF regulation/supervision in Bermuda were considered in this analysis.

[39] These typologies were pulled from typology reports and studies spanning a period from 2011 - 2019, published or circulated within organisations such as the FATF, Egmont Group, MENAFATF. MENAFATF is the FATF Style Regional Body (FSRB) for the Middle East-North Africa region

Back to Table of Contents

With the exception of the Banking, MSB and NPO sectors, the threat of TF occurring in each of the other sectors and channels was rated as LOW. For the most part, these ratings are consistent with the TF Threat findings in 2016, though in relation to CSPs the rating improved from medium-low to low, due to the fact that none of the typologies feature this sector as playing a role in TF at a global level.[40] In the case of TSPs, Lawyers, Accountants, Investment Funds/ Managers and DPMS, the rating was also mostly attributed to the fact that none of them featured in any of the international TF typologies, and that they did not appear in any TF-related evidence or intelligence, or any suspicion of TF occurring in Bermuda.

BANKING: Rating MEDIUM-LOW

Bermuda's banks process a high volume of sophisticated international transactions daily, particularly given its status as an international financial centre. Accordingly, it was very important that the potential TF threats to Bermuda's banking sector should be closely examined. Also, globally within the banking sector the typologies show it is typically the staple, less complex services which banks offer that could be targeted to move funds for TF purposes, e.g. wire transfers, debit/credit cards, misuse of charity accounts for non-charity activities.

Following the analysis of all relevant factors, the TF threat to Bermuda's banking sector was assessed as medium-low, the same as in 2016. This rating took into account that there are only four banks in Bermuda, none of which act as a correspondent bank. There was also a lack of evidence of TF in the sector. Any previous intelligence or investigations based on institutions' vigilance and SARs submissions, and in cooperation with foreign law enforcement and intelligence counterparts, ultimately confirmed that the suspicious transactions were legitimate.[41] In addition, there continued to be no evidence of any radicalised residents in Bermuda, or threat of domestic terrorism, that could drive TF activities within the local banking sector.

MONEY SERVICE BUSINESSES: Rating MEDIUM-LOW

International TF typologies show that globally, MSBs are used as a main channel for moving funds to support aspects of terrorist operations, both within countries

[40] In addition, in 2016 the CSP sector was still not subject to AML/ATF supervision and given the limited knowledge about whether appropriate controls were in place in this sector to monitor for, identify and report suspicious activities, it was challenging to rule out the likelihood of their involvement in TF in Bermuda or elsewhere. This is no longer the case and the absence of any TF cases, SARs or other intelligence sources to indicate their involvement in TF in Bermuda, this was also factored in the rating in 2020.

[41] See paragraphs 233 – 235, Bermuda's 2020 Mutual Evaluation Report, http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/CFATF-Mutual-Evaluation-Report-Bermuda-2020.pdf

Back to Table of Contents

and across multiple countries.[42] Often MSBs are used as a key component in large but simple funding networks, which enable multiple small donations to be made by numerous donor sources, channeled to a limited number of persons through the MSB systems.

In Bermuda, there are only three licences issued in the money service business sector, of which two licensees conduct remittances. The MSBs predominantly process outward remittances. A large component of the customer base is guest workers who rely on MSBs to regularly send funds to their home countries. From a TF threat perspective, it is relevant that some guest workers are from jurisdictions regarded to be higher risk for terrorism or TF. However, guest workers in Bermuda are subject to a stringent work permit process prior to entering the country.

The NRA analysis and findings from examining global typologies in which MSBs were featured rated the TF Threat for Bermuda's MSB sector as MEDIUM-LOW. This is lower than the medium rating in 2016, based on the following:

- The Bermuda Monetary Authority carefully controls market entry of MSBs through its robust licensing and evaluation process. Also, legislation requires MSBs to conduct due diligence and risk assessments of potential clients prior to conducting any transaction, as well as ongoing monitoring of client transactions.

- Given the unique context of this sector in Bermuda, it was determined that Bermudian MSBs are unlikely to be a central part of a TF funding network, as seen in the typologies (though it is acknowledged that donations into an existing foreign network could possibly be made through a local MSB).

- In Bermuda, MSBs have no agents or branches, ruling out one of the main features of MSB-based TF funding networks, namely, the ability to transfer donations from person to person in the same country via an MSB.

- There was no evidence of a domestic terrorism threat or radical ideology in Bermuda, whether amongst the local population or amongst the highly-vetted foreign/guest-worker population.

- The typologies show that use of MSBs is one of the main funding mechanisms for FTF recruitment, training and travel. There is no evidence of FTFs originating from Bermuda.

[42] In the international TF typologies assessed – see Annex II – MSBs featured in typologies E, F (3 of the 4 subcategories) and I.

Back to Table of Contents

NON-PROFIT ORGANISATIONS: Rating MEDIUM-LOW

There are several potential threats related to charities being used to support TF, including:

- Charities with international operations sending funds overseas and subsequently diverting funds for terrorist financing
- Unregistered churches receiving donations that are sent overseas as charitable donations to support terrorists
- Individuals conducting public fundraising for TF purposes under the auspices of a charity
- Misusing NPOs for training and recruitment of FTFs

The majority of the charities in Bermuda were determined to be exposed to a LOW threat from TF. This was because approximately 90% of Bermuda's 300 registered charities provide funding for charitable services solely within Bermuda to the local community. This is important given the finding of Low threat of terrorism activity in Bermuda and the absence of radicalisation, making it extremely unlikely that NPOs targeting funds domestically will be misused to support domestic terrorist activity, recruitment or radicalisation.

Bermuda's privately-funded charities that are exempt from registration are likely to focus on charitable activities overseas. However, there is no evidence, based on the intelligence and international cooperation requests to competent authorities, that Bermuda entities have been used to provide TF outside of Bermuda. Specifically in relation to NPOs as a possible source of TF, reference was made to the strong framework of supervision and the robust understanding of the operations and risks of the entities in this sector. This assessment was corroborated by the findings in Bermuda's 2020 MER in relation to Recommendation 8 [43] and Immediate Outcome 10.[44] Exempted charities are likely to have sophisticated operations to evaluate the persons and entities who receive their funds; therefore they would also have appropriate control mechanisms to minimise abuse/diversion of those funds. Exempted charities are also required to be clients of a licensed trust or corporate service provider, who must perform customer due diligence on the beneficial owners of the charities.

Closer consideration was given to any heightened TF threats to the approximately 10% of Bermudian NPOs directing funds to foreign charitable purposes.

[43] See TC Annex (pgs. 159 - 161), Bermuda's 2020 Mutual Evaluation Report, January 2020

[44] See Chapter 4 (pgs. 68 – 73), Bermuda's 2020 Mutual Evaluation Report, January 2020

Back to Table of Contents

This examination focused particularly on funding going to countries that may be at higher risk of terrorism or TF. The analysis found that the majority of causes these charities support are in countries considered to be at low risk for Terrorism or TF. It was also acknowledged that TF threat exposure can potentially be controlled for private charities via their CSPs relationships, i.e. if CSPs actively help manage TF risks by conducting monitoring and due diligence on the TF risk-profile of foreign beneficiaries, or vetting the countries in which charitable activities take place.

Given the lower TF threat to most Bermuda charities and the potential exposure of a few charities, and the global risks examined in the international TF typologies, the TF threat rating for this sector was MEDIUM-LOW. This is improved from the 2016 rating of Medium. The improved rating is due partly to the significant increase in knowledge about the operations and exposure of the sector, based on substantial risk identification and mitigation work conducted within the sector since 2016.

INSURANCE: Rating LOW

There was no local investigation nor any intelligence, whether sourced locally or internationally, which indicated any involvement of this sector in TF. This finding applied for both the Long-term (life) and General Business segments of the sector, the latter representing over 90% of total assets in Bermuda's market. A key feature of the General Business segment in particular remains insurance products that have no cash surrender value and no payouts once policies mature; this makes Bermuda's insurance sector less attractive for moving terrorist-related funds. It was therefore determined that the rating of Low was appropriate for this sector.

In addition, the nature of the global TF typologies in which the insurance sector was featured related to threats such as piracy for ransom (PFR) and kidnap for ransom, and none involved Bermuda insurers. PFR as a form of TF is substantially diminished on the global level, significantly reducing Bermuda's potential exposure to this TF risk. Only a handful of Bermuda companies underwrite business lines that expose them to kidnapping claims; there was no evidence of misuse of insurance policies for payments related to such claims that benefited terrorists.

The Low rating is the same as in 2016. However, it should be noted that the Bermuda authorities remain alert to other types of insurance coverage, such as for cyber attacks, which could potentially be used for TF purposes.

Back to Table of Contents

DIGITAL ASSET BUSINESSES: Rating LOW

Bermuda has taken a proactive approach and has enacted legislation to create a robust regulatory framework for Digital Asset Issuance[45] and Digital Asset Businesses. The sector did not exist in Bermuda during the 2016 NRA reporting period. Digital assets (e.g. virtual currencies) have subsequently featured in a few recent global typologies; Bermuda's 2020 NRA focused for this report on the use of wallets and virtual currency to make donations supporting terrorism-related activities, persons or organisations.

On that basis, the analysis determined that the potential TF threat to this sector in Bermuda was limited. During the reporting period only four licensees were operating in or from Bermuda, two with full licences and two with modified licences. Of the two full licensees, only one was operational. The other does not conduct the kind of business that would expose them to the threats described in the typologies, namely the offer of wallet or exchange services. Of the other two modified licensees, only one of them has clients and it does not offer wallet services or other transactional services that could expose it to such threats.

Given the TF methods and techniques shown by the typology to be used in the abuse of this sector for TF and the mitigants specified above, it was determined that the rating of Low is appropriate for this sector at this time.

CASH COURIERS: Rating LOW

The use of cash couriers is often seen in the international TF typologies, especially connected to movement of funds by Foreign Terrorist Fighters (FTF).[46] Although there are examples in Bermuda of money laundering cases involving the use of cash couriers, the findings in the Terrorism Threat assessment had to be considered in determining the threat associated with this channel of TF in Bermuda. It was determined that the absence of radicalisation in Bermuda, together with the waning incidence of FTFs travelling from the West into conflict areas, significantly reduce the likelihood of this TF method occurring in Bermuda.

Accordingly, the Low rating in relation to cash couriers was justified on these grounds; and is also the reason for the change in rating from medium-low in 2016.

[45] Also known as Initial Coin Offering (ICO).

[46] Typologies D, E and F in Annex II, strongly demonstrate the role played by Cash Couriers in the financing of terrorism. The most prolific use of this method of movement of funds across borders was seen in relation to three of the four categories considered in typology F, regarding Foreign Terrorist Fighters (FTFs). Movement of cash across borders by means of couriers was also shown in the Maritime Piracy for Ransom (PFR) cases and the Kidnap for Ransom (KFR) cases.

Back to Table of Contents

Other Channels seen in the Typologies – HAWALAS

Given the wide use of Hawalas in international TF typologies, the assessment considered whether there was any evidence that such activities, or other similar informal money transfer systems, are taking place in Bermuda. Hawalas are a form of a traditional banking system originating in the Middle East, Africa and certain parts of Asia. It is based on an extensive honour system and involves the transfer of money from one person to another, without any actual movement of funds. The system works through an informal underground network, involving a handler accepting cash from a customer in one country/location, who communicates this information to a handler in the intended recipient's country/location. That handler will pay out the equivalent amount (minus a commission) to the recipient.

Local authorities in Bermuda are satisfied that to the best of their knowledge there are no Hawalas or other unregulated money transfer or banking systems operating in Bermuda. Any business offering "money or value transfer services",[47] would be subject to AML/ATF regulation in Bermuda. Further, the provision of "money transmission services" or "payment service business" would bring a business under prudential regulation[48] requiring a licence. No such Hawala businesses are currently licensed and regulated by the BMA, nor is the BMA aware of any unlicensed activity of this kind. Bermuda's highly formalised economy and apparent high level of financial inclusion also heavily mitigate against this type of activity. Furthermore, as a small society with close-knit communities, it would be highly unlikely for such activities to exist and be hidden from the authorities if they were happening.

[47] Proceeds of Crime Act 1997, Schedule 3, 1(d).

[48] Money Service Business Act 2016, 2 (2) (a) and (d)

Back to Table of Contents

Conclusion

The 2020 TF NRA analysis of directions, sources and channels of funds (supported through the analysis of international typologies), determined that an overall rating of Low for Terrorist Financing threats to Bermuda was appropriate. This is the same as in 2016. While there is no evidence for Bermuda being a source of TF, the jurisdiction has continually strengthened its ATF framework to ensure that the regime remains robust and is able to adapt appropriately to any emerging TF threats.

A careful examination of a broad spectrum of international TF typologies confirmed that the threat of TF is also low across the relevant sectors, other than the banking, MSB and NPO sectors. This finding is also supported by there being no confirmed cases of TF in Bermuda. Regarding the banking, MSB and NPO sectors, the international typologies indicated a marginally higher exposure to TF. However, the TF threat is lowered for these sectors particularly when considered in light of the terrorism threat findings. Also, there has been no domestic or foreign-sourced intelligence to suggest that terrorism financing has occurred in Bermuda in any sector, whether to support domestic or foreign terrorist activity or as a transit point to move funds from one country to another.

Despite these findings the Bermuda authorities remain vigilant and recognise that no jurisdiction is completely immune to TF threats and terrorist activities. Therefore, Bermuda's long-standing commitment and contributions to global ATF initiatives remains active and strong. The relevant Bermuda agencies are also fully committed to regularly assessing terrorism and TF threats, while ensuring the jurisdiction's ATF regime remains robust, adaptable to address ever-evolving risks and aligned with international standards.

Back to Table of Contents

Chapter 24: Conclusion

Bermuda's third National Risk Assessment on Money Laundering commenced in 2020 and was concluded in 2021; and its second National Risk Assessment on Terrorism Financing was conducted in 2020. The competent authorities continued to build on the excellent foundation laid in the three prior NRAs conducted in 2013, 2016 and 2017, leveraging their greater experience and the availability of relevant and comprehensive data for all aspects of the assessments, to ensure a high quality and credible outcome.

The Money Laundering Risk in Bermuda

The National ML Threats was determined to be HIGH. As previously noted, the assessment of the national ability to combat ML, as well as the effectiveness of the controls in place at the sectoral level, confirmed the robustness of Bermuda's AML framework, as is reflected in Bermuda's 2020 Mutual Evaluation Report.[49] Threats from abroad still remain more severe than domestic ML threats. However, more foreign-based predicate offences ranked as high threats in the 2020 NRA. It was also recognised that international proceeds of crime laundered in Bermuda would typically be larger in scale and consequently be rated as higher-threat. The assessment also showed some potential for increased domestic sources of ML, but drug trafficking remained the highest ML threat domestically. More comprehensive data and information also enabled a complete assessment of cross-border threats to the jurisdiction.

There are ongoing enhancements and effectiveness in the national AML/ATF framework, even as the ML threat landscape shifted. Overall, as evidenced in the 2020 Mutual Evaluation Report, this NRA again confirmed that Bermuda has sound systems and structures in place in respect of AML policy and strategy, the legal framework for ML, sectoral regulation and oversight and international cooperation. Focus will remain on facilitating resources in these areas, as well as for financial intelligence sharing, detection and investigation of predicates and of ML, and recovering proceeds of crime.

Inherent Money Laundering Risk at the Sectoral Level

Once again the National Risk Assessment included the assessment of sectoral threats and sectoral inherent vulnerabilities, resulting in inherent ML risk ratings for each sector. The assessment of ML threats affecting each of the regulated sectors is part of the assessment of national threats. The updated conclusions for Bermuda's national and sectoral risk ratings will allow Bermuda's competent authorities, policy makers and private sector stakeholders to have a current understanding of money laundering risk, and to appropriately tailor their policies, procedures, resources and combating strategies to manage the risk.

The table below shows the 2020 results for the 16 sectors assessed, including the underlying threat and inherent vulnerability ratings which led to those results.

[49] https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/CFATF-Mutual-Evaluation-Report-Bermuda-2020.pdf

Back to Table of Contents

Table 8: 2020 results for Sector Assessment

Sector	2020 ML Threat Rating	2020 Inherent Vulnerability Rating	2020 Inherent ML Risk Rating
Deposit Taking	HIGH	MEDIUM	MEDIUM-HIGH
Securities	HIGH	MEDIUM-HIGH	HIGH
AML/ATF Regulated Insurance	MEDIUM-HIGH	MEDIUM	MEDIUM-HIGH
General Business & ReInsurance	LOW	MEDIUM-LOW	MEDIUM-LOW
Money Service Business	MEDIUM	MEDIUM	MEDIUM
Other Financials: Bermuda Stock Exchange	LOW	MEDIUM-LOW	MEDIUM-LOW
Lending	LOW	MEDIUM-LOW	MEDIUM-LOW
Trust Service Providers	HIGH	HIGH	HIGH
Corporate Service Providers	HIGH	MEDIUM-HIGH	HIGH
Accounting Sector	LOW	MEDIUM	MEDIUM-LOW
Legal Sector	HIGH	MEDIUM-HIGH	HIGH
Real estate	MEDIUM	MEDIUM-HIGH	MEDIUM-HIGH
Casino Gaming	LOW	MEDIUM	MEDIUM-LOW
Dealers in precious metals and stones	MEDIUM-LOW	MEDIUM	MEDIUM
Betting	MEDIUM	MEDIUM	MEDIUM
High Value Goods Dealers (Cars, bikes and boats)	LOW	MEDIUM-LOW	MEDIUM-LOW

Terrorist Financing Risk Assessment

It remains that there is no evidence of terrorism or terrorism financing threat to Bermuda. Domestic, regional and global threats of terrorism to Bermuda were all assessed to be low. There was also no evidence of Bermuda being either a source of TF, or transit point for such criminal activity.

Based on the examination of international TF typologies in this assessment, **the sectoral threat of TF is also LOW in Bermuda,** other than in the banking, MSB and NPO sectors. This finding is also supported by the absence of any confirmed cases of TF in Bermuda. The assessment showed that the banking, MSB and NPO sectors had a higher exposure to TF, but in the context of the national threat findings overall, and specific factors in those sectors unique to Bermuda, the TF threat is reduced. However, there is no complacency about these results. Bermuda's authorities will continue to remain vigilant, take steps to share any terrorism-related intelligence and to work cooperatively to keep the threat of terrorism at bay.

Back to Table of Contents

Subsequent Events

The assessment period covered by both the ML and TF NRAs was January 1, 2017 to December 31, 2019. The following represents a documentation of the regime changes and progress made by the authorities since 2020, all of which has been articulated to the CFATF in Bermuda's first Follow-Up Report, presented to the CFATF Plenary in May 2022:

1. The Registrar of Companies (Supervision and Regulation) Act 2020 was enacted in July 2020, and came into force on 1st November 2020. Through amending the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008, this Act transferred the responsibility for the supervision of Dealers in High Value Goods from the FIA to the Registrar of Companies; and empowered the ROC to be able to carry out these and other functions. This has enabled the FIA to focus all its resources on its core mandate of financial intelligence.

2. The Casino Gaming Act 2014 was substantially updated and its name changed to the Gaming Act 2014. This also resulted in a name change for the Commission also, to the Bermuda Gaming Commission. The amendments became operational on 1st August 2021.

3. The Betting Act 2020 was enacted in June 2021 and came into operation on 1st August 2021. This Act repealed the Betting Act 1975 and replaced the Betting Licensing Authority with the Bermuda Gaming Authority as the regulator for betting operations, with enhanced powers and responsibilities.

4. The Proceeds of Crime Amendment Act 2022 was enacted on 27th February 2022, and amended the Proceeds of Crime Act and Regulations. The amendments enhanced the AML/ATF controls in relation to digital assets and digital asset businesses, by implementing the "travel rule" and the few outstanding requirements in Recommendation 15 of the FATF Standards, which the FATF added after Bermuda's mutual evaluation.

Back to Table of Contents

Appendix A. Glossary

AG	Attorney-General
ALC	Authorisations and Licensing Committee (BMA)
AMEX	American Express
AML	Anti-Money Laundering
AML/ATF Board	Barristers and Accountants AML/ATF Board
ARI	AML-Regulated Institution
ATFA	Anti-Terrorism (Financial and Other Measures) Act 2004
ATF	Anti-Terrorist Financing
AUM	Assets Under Management
BALT	Bermuda Association of Licensed Trustees
BerDIN	Bermuda Drug Information Network
BILTIR	Bermuda International Long Term Insurers and Reinsurers
BIMA	Bermuda Insurance Managers Association
BIRBA	Bermuda Insurance and Reinsurance Brokers Association
BMA	Bermuda Monetary Authority
BPS	Bermuda Police Service
BSX	Bermuda Stock Exchange
BSX <GO>	Bloomberg
BVI	British Virgin Islands
CDD	Customer Due Diligence
CFATF	Caribbean Financial Action Task Force
CFT	Combatting the Financing of Terrorism
CPA Act	Chartered Professional Accountants of Bermuda Act 1973
CPA Bermuda	Chartered Professional Accountants Association of Bermuda
CSP	Corporate Service Provider
CTR	Cash Transaction Reports
DAB	Digital Asset Business
DNFBP	Designated Non-Financial Businesses and Professions
DPMS	Dealers in Precious Metals and Stones
DPP	Department of Public Prosecutions
EFTs	Electronic Funds Transfers
EU	European Union
FATF	Financial Action Task Force
FCO	Foreign and Commonwealth Office
FDI	Foreign Direct Investments
FIA	Financial Intelligence Agency
FIU	Financial Intelligence Unit
FT	Financing of Terrorism

Back to Table of Contents

FTF	Foreign Terrorist Fighters
GDP	Gross Domestic Product
GWP	Gross Written Premium
HNWI	High Net Worth Individuals
HVD	Dealers in High Value Goods
IAIS	International Association of Insurance Supervisors
IBA	Investment Business Act 2003
IFA	Investment Funds Act 2006
IFC	International Financial Centre
ILS	Insurance Linked Securities
IM	Insurance Managers
IOSCO	International Organization of Securities Commissions
IRI	Incoming Request for Information
KYC	Know Your Customer
LLC	Limited Liability Company
LPI	Limited Purpose Insurer
LSE	London Stock Exchange
LTD	Long-Term Direct
LT Insurance	Long-Term/Life Insurance
MER	Mutual Evaluation Report
ML	Money Laundering
MLA	Mutual Legal Assistance
MoU	Memorandum of Understanding
MSB	Money Services Business
NAMLC	National Anti-Money Laundering Committee
NAV	Net Asset Value
NLP	Non-Licensed Persons
NPO	Non-profit Organisation
NPW	Net Premiums Written
NRA	National Risk Assessment
NTWG	National Threats Working Group
NVWG	National Vulnerabilities Working Group
NYSE	New York Stock Exchange
OECD	Organisation for Economic Cooperation & Development
ORI	Outgoing Request for Information
OTC	Office of the Tax Commissioner
PCA	Police Complaints Authority
PEP	Politically Exposed Person

Back to Table of Contents

PF	Proliferation Finance
POCA	Proceeds of Crime Act 1997
POC Regulations	Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008
PTC	Private Trust Company
REBLA	Real Estate Brokers' Licensing Act 2017
RFI	Regulated Financial Institution
RPF	Regulated Professional Firm
SAR	Suspicious Activity Report
SEA Act	Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008
SFR	Statutory Financial Return
SORE	Superintendent of Real Estate
SPI	Special Purpose Insurer
STR	Suspicious Transaction Reporting
TAFA	Terrorist Asset-Freezing etc. Act 2010
TCSP	Trust or Company Service Provider
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
TIEAs	Tax Information Exchange Agreements
TSP	Trust Service Provider
UAE	United Arab Emirates
UK	United Kingdom
UN	United Nations
US	United States
UNSCR	United Nations Security Council Resolution
USD	US Dollar
WB	World Bank
WG	Working Group

Back to Table of Contents

Appendix B. The World Bank Tool – Money Laundering Risk

As noted in Chapter 4 of this report, the 2020 risk assessment was conducted using the World Bank Model's seven (7) ML modules, namely:

MODULE 1 - National Money Laundering Threat;

MODULE 2 - National Vulnerability;

MODULE 3 - Deposit-Taking (Banking/Credit Union) Sector Vulnerability;

MODULE 4 - Securities Sector Vulnerability;

MODULE 5 - Insurance Sector Vulnerability;

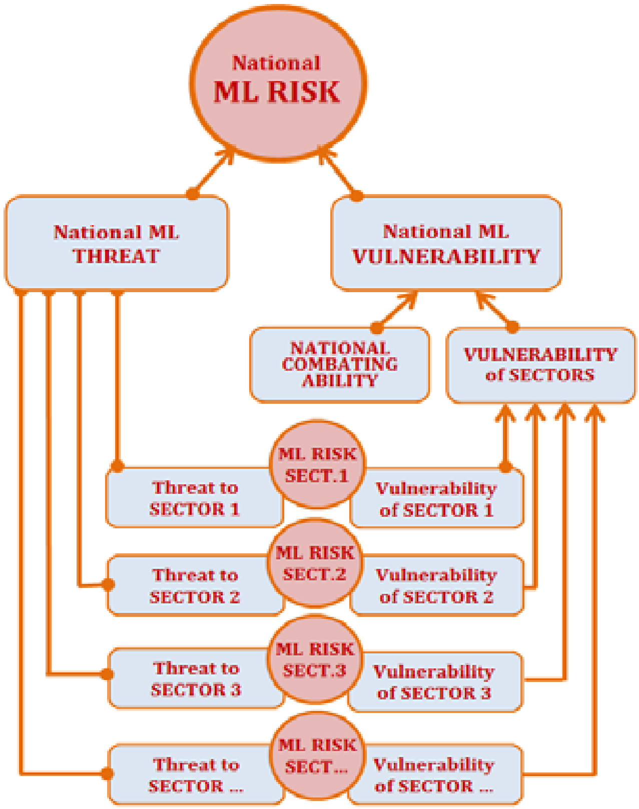
MODULE 6 - Other Financial Sectors Vulnerability – namely, Money Service Business and Stock Exchange, and;

MODULE 7 - Non-Financial Sectors Vulnerability – namely Designated Non-Financial Businesses and Professions (DNFBPs) and others, that is:

- Trust Service Providers;
- Corporate Service Providers;
- Casino Gaming;
- Real estate dealers;
- Lawyers;
- Accountants;
- Dealers in Precious Metals and Stones;

Other Dealers in high value goods – cars, boats, bikes, antique dealer and auctioneers; and Betting shops.

The figure below shows the relationship between the modules:



How Does the Tool Work?

The World Bank Model has a highly integrated modular methodology that works as follows:

i. **Each of the Modules that assess vulnerability (Modules 2 – 7) is broken down into intermediate variables and input variables.** Each input variable assesses various key features of the sectoral or national AML framework or the products offered by each sector; and require a quantitative assessment to be made about them by the Working Groups. Based on the scores determined for the input variables, the intermediate variables are calculated by the Model itself, using its proprietary algorithms.

ii. **The combination of input and interme-**

Back to Table of Contents

diate variables generates a single quantitative score for each vulnerability module (Modules 2 – 7). These scores translate into the 5-point vulnerability ranking of 'Low', 'Medium-Low', 'Medium', and 'Medium-High' or 'High'. This applies for both sectoral and national vulnerability assessments.

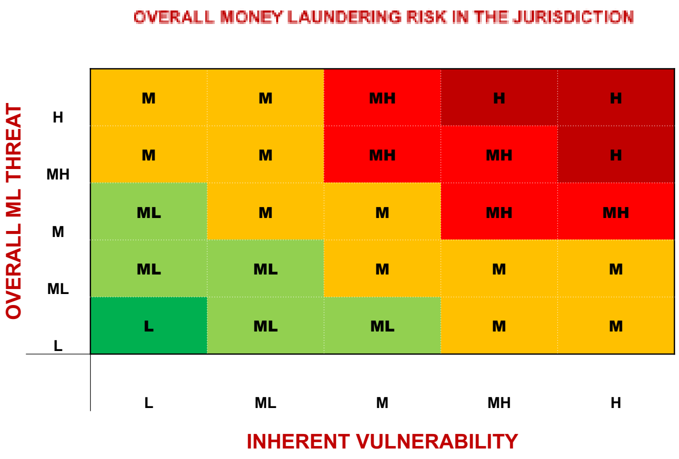
iii. **The single resulting quantitative score generated for each of the sectoral assessments, using Modules 3 to 7, are in turn fed into Module 2 on National ML Vulnerabilities, in order to generate a single quantitative score that indicates the national vulnerability level.** The national vulnerability score that is obtained can then be plotted to a 5-point national vulnerability rank which will be 'Low', 'Medium-Low', 'Medium', 'Medium-High' or 'High'.

iv. **Module 1 on National ML Threats does not operate on quantitatively determined input variables.** Instead, the module requires the Working Group to determine a subjective ranking of the ML threat from the various predicate offences into 'Low', 'Medium-Low' 'Medium', 'Medium-High' or 'High'. The module also requires the ranking of the ML threat to each sector, as well as the identification and ranking of the cross-border threat, using the same ranking levels of 'Low', 'Medium-Low' 'Medium', 'Medium-High' or 'High'. Further, upon ranking all of these threats, the Working Group is required to determine a single national threat rank, which will also be either 'Low', 'Medium-Low', 'Medium', 'Medium-High' or 'High'.

v. **Finally, the World Bank model provides a matrix in the form of a heat map (see below) to combine the rankings of Modules 1 (National ML Threats) and 2 (National ML Vulnerabilities) in order to generate an overall ML risk for the country.** This same matrix can be used to generate the overall sectoral risk ratings, using the vulnerability rankings generated by Modules 3 – 7 for the sectoral assessments and the sectoral threat rankings generated using Module 1.

The figure below illustrates the threat/ vulnerabilities matrix and the risk levels have been colour-coded, with lower levels being depicted in shades of green, medium level depicted in yellow, and the higher levels depicted in red.

Figure 4: Risk Heat Map - threats and vulnerabilities matrix



OVERALL MONEY LAUNDERING RISK IN THE JURISDICTION

OVERALL ML THREAT					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

INHERENT VULNERABILITY

Back to Table of Contents

Appendix C. Working Groups for 2020 Money Laundering Threat and Vulnerability Assessments

i. **National Threats Working Group** – representatives from the Attorney-General's Chambers, the Bermuda Monetary Authority, the Bermuda Police Service, the Customs Department, the Department of Public Prosecutions, the Financial Intelligence Agency, the Ministry of Finance and the Office of NAMLC (Chair). Specific assistance was sought and received from the Department of Statistics, the Office of the Tax Commissioner and the Department of Immigration.

ii. **National Vulnerability Working Group** – representatives from the Attorney- General's Chambers, the Bermuda Monetary Authority, the Bermuda Police Service, the Customs Department, the Department of Public Prosecutions, the Financial Intelligence Agency, the Ministry of Finance, the Office of NAMLC (Chair), the Office of the Tax Commissioner, the Judiciary, the Registrar of Companies, the Registry General and the Ministry of Legal Affairs and Constitutional Reform. Specific input was also solicited from CPA Bermuda and the Bermuda Public Accountability Board.

iii. **Banking Sector Working Group** – representatives from the Bermuda Monetary Authority (AML Supervision team, Banking Prudential Supervision team, legal and policy representatives, licensing and authorization representatives, and the financial stability representative). In addition, Working Group discussions were held with the Bermuda Bankers Association Compliance Sub-Committee.

iv. **Securities Sector Working Group** – representatives from the Bermuda Monetary Authority (AML Supervision team, Insurance Prudential Supervision team, legal and policy representatives, licensing and authorization representatives, and the financial stability representative). In addition, Working Group discussions were held with licensees regulated by the Investment Funds Act, licensees regulated by the Investment Business Act and lawyers that deal with non-licensed persons. As there was no association or collective group of representatives for this industry sector or any sub-sectors, all licensees were invited to participate.

v. **Insurance (AML/ATF Regulated) Sector Working Group** – representatives from the Bermuda Monetary Authority (AML Supervision team, Insurance Prudential supervision team, legal and policy representatives, licensing and authorization representatives, and the financial stability representative). In addition, Working Group discussions were held with the Bermuda International Long Term Insurers and Reinsurers (BILTIR), Bermuda Insurance Managers Association (BIMA) and the Bermuda Insur-

Back to Table of Contents

ance and Reinsurance Brokers Association (BIRBA) on inherent vulnerability variables and on select general input variables.

vi. **Lending Sector Working Group** – representatives from the Bermuda Monetary Authority (AML Supervision team, legal and policy representatives, licensing and authorization representatives, and the financial stability representative). In addition, Working Group discussions were held with operators in the sector.

vii. **General Business & ReInsurance Sector Working Group** – representatives from the Bermuda Monetary Authority (AML Supervision team, Insurance Prudential supervision team, legal and policy representatives, licensing and authorization representatives, and the financial stability representative). In addition, Working Group discussions were held with the Association of Bermuda Insurers and Reinsurers (ABIR), Bermuda Insurance Managers Association (BIMA) and the Bermuda Insurance and Reinsurance Brokers Association (BIRBA) on inherent vulnerability variables and on select general input variables.

viii. **BSX Sector Working Group** – representatives from the Bermuda Monetary Authority (AML Supervision team, BSX Prudential Supervision team, legal and policy representatives, licensing and authorization representatives, and the financial stability representative). In addition, Working Group discussions were held with the BSX.

ix. **Legal Sector Working Group** – representatives from the Barristers and Accountants AML/ATF Board, the Bermuda Bar Association and lawyers from industry.

x. **Corporate Service Providers Working Group** - representatives from the Bermuda Monetary Authority (AML Supervision team, legal and policy representatives, and the financial stability representative). In addition, Working Group discussions were held with representatives from industry (small entities to large and long established businesses) on inherent vulnerability variables and select general input variables.

xi. **Trust Service Providers Working Group** - of representatives from the Bermuda Monetary Authority (AML Supervision team, legal and policy representatives, and the financial stability representative). In addition, all representatives within the trust sector were invited to participate and Working Group discussions were held with the Bermuda Association of Licensed Trustees (BALT).

Back to Table of Contents

xii. **Accounting Sector Working Group** - representatives from the Barristers and Accountants AML/ATF Board, the Chartered Professional Accountants (CPA) of Bermuda, members of CPA Bermuda, and other accountants from industry.

xiii. **Real Estate Sector Working Group** - representatives from the Office of the Superintendent of Real Estate, representatives from the Real Estate Division of the Chamber of Commerce, and independent representatives from the real estate sector.

xiv. **High Value Dealers Sector Working Group** - representatives from the Registrar of Companies. Discussions were held with representatives from the sector.

xv. **Casino Gaming Working Group** - representatives from the Bermuda Gaming Commission and the Office of NAMLC.

xvi. **Dealers in Precious Metals and Stones Sector Working Group** - representatives from the Registrar of Companies. Discussions were held with representatives from the sector.

xvii. **Betting Sector Working Group** - representatives from Bermuda Gaming Commission, Bermuda Betting Licensing Authority, the Office NAMLC and representatives from several operators within the betting sector.

Back to Table of Contents

Appendix D. International Typologies used as part of Terrorist Financing Assessment

The typologies below were extracted from typology reports and studies published or circulated within organisations such as the FATF, Egmont Group, MENAFATF[50] and other FATF-style regional bodies, spanning a period from 2011 - 2019. The typologies allowed the Working Groups to identify and analyse various TF methods and techniques known to be used globally, and determine whether and how such methods and techniques might occur in sectors within Bermuda. Accordingly, the assessment of the sectoral TF threats is an assessment of likelihood and potential, rather than an assessment based on actual quantitative or qualitative data of TF occurring in these sectors.

In considering the TF typologies, it became clear that unlike in money laundering typologies, many sectors in Bermuda have not been featured in these global TF transactions described in the typologies. Nonetheless, an assessment was still conducted on all relevant Bermuda sectors, to determine whether any domestic or foreign-sourced intelligence that was specific to Bermuda could assist in evaluating the TF threat posed by them.

1.

Typology A: Case of potential recruitment to a terrorist organisation

(Case No. 16)

Key judgments

Person is likely using his position as a religious leader and founder of religious charities to promote an extremist interpretation of a religion in Australia, and is possibly encouraging Australia-based entities to travel to Syria and Iraq to fight for ISIL.

Person A came to AUSTRAC's attention due to adverse media attention. Person A appears in multiple media articles due to his position as a self-proclaimed religious leader who preaches extremist ideology in Australia.

Extrinsic data holdings link Person A to persons that are considered a national security risk, including persons that have travelled to Syria and Iraq to join ISIL. Further intelligence, which could not be revealed for the purposes of this report, suggests links between Person A and activities to recruit individuals to join terrorist organisations.

Extrinsic data holdings and open source link person A to a known Australia-based extremist person B. Persons A and B belong to the same prayer group. They are co-founders of an unregistered charity, Charity A, which is focused on servicing a particular religious community.

Charity A's Facebook page also linked the charity to another unregistered religious charity, Charity B.

Due to the manner in which Charity A and B were collecting donations, primarily through domestic transfers and credit card payments, AUSTRAC has no visibility of the transactions. Given the high-risk individuals involved in these charities, and the

[50] MENAFATF is the FATF Style Regional Body (FSRB) for the Middle East-North Africa region.

Back to Table of Contents

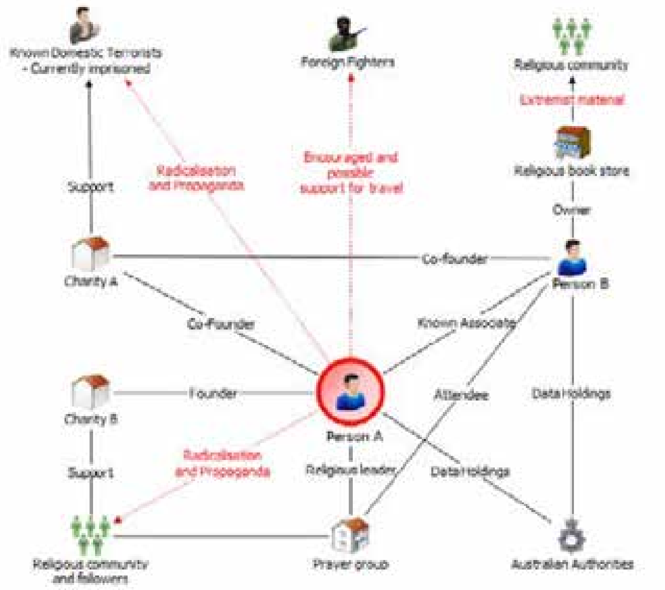
limited regulatory oversight, AUSTRAC assessed it was possible that the charities used some of the funds collected for non-charitable causes – including promoting extremism, and supporting events where extremist ideologies are preached and where the risk of terrorist financing is higher.

Charity A and B appear to be conducting legitimate transactions supporting a religious community in Australia. The financial support they provide to the community may endear them to the marginalised members of this community, possibly sowing the seeds for radicalisation.

There are limited reportable transactions of the persons and charities. It is possible the persons are using alternate methods of banking to avoid scrutiny of their financial activities. This could include cash transactions below the reportable requirement, using cash couriers to move funds domestically and internationally, the use of identify fraud or using family members.

Figure 1: Network Diagram of Case of Possible Radicalisation and Propaganda

Source: Australia



Typology B: Bank account of a charity used to send money to the Philippines

(Case No. 62)

Summary of Activity: The bank account of a charity in Country A was used to send money to the Philippines. The charity located in the Philippines was, unknown to the Charity A charity, acting under coercion of a terrorist organization. In February 2017, the charity began to raise money for charitable purposes in the Philippines. The money, much of which was provided by Filipino residents in Country A, was sent to a bank account in one of the largest cities in the Philippines, A City. A City, at that time, was a stronghold of forces and militants affiliated with the Islamic State of Iraq and the Levant (ISIL) and jihadist groups.

Financial Analysis:

- Funds were being sent to The Philippines by local residents to assist those in need in the war torn area. These funds were forcefully intercepted by the terrorist groups in the Philippines when the affiliated charity in the Philippines received the funds.
- Large cash deposits were noted on charity's bank account in Country A; however, the source of these funds was unclear as cash deposits were accepted.

Back to Table of Contents

Data Overview

Type or terrorism: Relation of FTF

Used means: None

Targets: None

Statement: None

Claimed: No

Connections: Close contact of number of FTFs and other radical persons

Financial products: Use of bank account of a Bermuda charity

SAR reporting: Extensive reporting by local banks during and after terrorist stronghold, using ML/TF indicators

Possible financial indicators:

- Sudden influx of donations towards a terror-driven area of the Philippines via a charity's bank account in Country A.

Typology C: TF and Virtual Currencies

(Cases Nos. 6 & 7, 29 – 34 & 61)

Jihadist actors have been identified engaging in crypto-currency-enabled fund-raising activities through ostensible charities, media/propaganda offices and other organisations.

One recently observed case is that of AS, an ostensible charitable and fundraising organization that claims to be supporting militants in Syria.

In December 2017, AS began posting calls on forums such as Telegram and Twitter for supporters to send Bitcoin to addresses/e-wallets controlled by the group. In early 2018 AS began posting on its Twitter account calls for supporters to send funds to the group through Bitcoin ATMs, and posted links to CoinATMRadar maps showing the locations of ATMs.

The group has also begun soliciting donations in three private coins, Monero, Dash and Verge. The group's site also includes an embedded Monero mining tool, allow visitors to the site to loan computer power to provide AS with newly minted Monero. The fact the group is looking to these coins as a funding source suggests they may have concerns about the transparency Bitcoin affords.

As the group has been dropped from social media platforms and from fundraising sites such as Patreon they have also switched to raising funds on extremist-run crowd-funding sites such as Hatreon or on Tor-based donation sites.

Another scheme being used by the group is to use stolen cards and compromised accounts to purchase crypto-currencies, which are then sold for fiat and transferred onward to accounts held in the names of front companies in high risk countries.

The group's e-wallets received transfers from multiple individuals, located in different countries. Money from the e-wallets was then sent to a mobile bank account linked to a phone number located in a conflict area. Web-hosting services were also purchased in Bitcoin from the e-wallets.

Back to Table of Contents

Analysis of Bitcoin payment flows linked to the e-wallet addresses indicate that some donations made to the organization ultimately trace back to BTC-e, suggesting that some jihadist supporters may attempt to exploit non-compliant exchanges when making donations (the US indictment of BTC-e and Alexander Vinik also indicates that aliases that illicit actors used to establish accounts at BTC-e included names such as 'ISIS'). Bitcoin block chain analysis also indicates that addresses associated with these donations have also sent funds to other unregulated exchanges, P2P exchanges and online gambling sites.

Further analysis has shown the use of Bitcoin to purchase airline tickets, as well as multiple transactions with a bitcoin-funded debit card, consisting of refunds and purchases with an airline over a 2 week period. The analysis also revealed payments sent to bitcoin wallets associated with two now defunct dark net marketplaces.

Source: Multiple

Typology D: Maritime (Civil Aviation) Typology

(Cases Nos. 47 – 51 - consolidated)

M.V. Anonymous Motor Vessel/Aircraft – was a vessel/aircraft registered in Country X. The vessel was en route to another country on the other side of the world. The cargo was of extremely high value and high security, and included numerous and various types of Soviet-made arms and ammunition. The vessel/aircraft was therefore targeted and hijacked by Somali pirates/hijackers, who threatened to blow up the vessel and kill the crew if a ransom of USD $XXXX was not paid. The vessel's ownership was not fully clear – a company with part-ownership was readily identifiable, but the other owner was a mystery. The insurers of the vessel engaged the services of an intermediary negotiator to negotiate with the pirates. In light of the nature of the pirates' threats and concerns about the safety of the crew, the governments of several concerned countries began to consider alternate means of re-taking the vessel/aircraft from the pirates/hijackers.

After some negotiation, but before the coalition of countries could mount a successful mission to retake the vessel/aircraft, a ransom was paid by the mystery owner to the pirates. The USD cash for the ransom (in millions) was withdrawn from a bank account in Country X in cash. Arrangements were made to deliver the cash to the pirates, who shortly released the vessel and crew.

It was later learned that a supplemental agreement had been arrived at through the efforts of the negotiator engaged by the insurance company to get the pirates to agree to a lower ransom. This required an additional amount of USD $XX to be paid to the pirates, via wire transfer to a bank account provided to them by the pirates' negotiator. The known part-owner of the vessel/aircraft subsequently arranged to have this supplemental amount wired from their bank account in Country X to the provided bank account in another country. It is understood that the insurer indemnified both owners for the full amount of the ransom paid.

Back to Table of Contents

Typology E: Kidnap and Ransom Typology

(Cases Nos. 53 – 55)

These typologies deal with the kidnapping threat to foreign nationals in high risk jurisdictions. Whilst this is a TF matter it should also be considered that the risk of kidnapping is not limited to high-risk jurisdictions. These three typologies highlight the associated risk of travel/work in high-risk destinations, which have a high level of kidnapping for ransom schemes.

Case one involves the kidnapping of a group of four Western tourists who were on holiday in West Africa. The tourists were returning home from a cultural event when their convoy was attacked. The hostages were taken to a neighbouring country B to evade local security forces. The terrorist organisation made an offer to the Government of one of the hostages for his release in exchange for a member of their group, who was under arrest, in addition to a ransom of approximately $13million. This offer was declined by that Government which resulted in the hostage being executed. The remaining 3 hostages were later released following another ransom demand however the specific terms of the release or if a ransom was actually paid is unknown.

In a similar incident, the same terrorist group kidnapped two foreign nationals while working for a relief agency in Country X. The group used a similar method of negotiating the release of one of their group leaders who was detained in a foreign country. The Governments of the two captives paid out a substantial amount of money through an intermediary. The intermediaries seized a large portion of the ransom money and paid a portion to the terrorist group. The victims were released from captivity and the leader and some followers were released from prison. Another case involves a foreign terrorist organisation operating out of the Philippines who were directed by their leader to engage in kidnappings for ransom in order to raise funds for the group and to raise the public's awareness of the group's purpose. Armed members of the group kidnapped 16 individuals, which included citizens of other countries. They forced the victims to march up a mountain in order to evade the authorities. Four days later, the hostages were released after a ransom was paid.

The kidnapper and members of his group were caught through rigorous efforts of law enforcement in tandem with the FIU which helped record and trace large bulk amounts of cash entering the banking system. The kidnapper was sentenced to 23 years in prison.

In the third case, an Iraqi known to workers in an NGO convinced members to travel with him to a specific location in Iraq as part of their NGO work. During the trip, one of the workers along with the Iraqi were kidnapped. A ransom was sent to a relative of the NGO worker who arranged for a six figure wire transfer to a bank in Iraq. While making the transfer, the customer informed the teller that the money was for a ransom payment, triggering the filing of a SAR.

Investigations revealed that the Iraqi was involved in an attempted extortion of money from a business associated with an FTO and may have provided some support to the organisation. The kidnapping was plotted in an effort to deal with his financial liabilities incurred when the extortion was discovered. The bank froze the funds and were advised not to release them as it may constitute terrorist financing. A ransom was eventually paid through other undetected means and the hostages released. Although the kidnapping was a criminal act, it was perpetrated by someone with terrorist connections and could have resulted in funds going to the group.

Sources: United Kingdom, Philippines and United States

Back to Table of Contents

Typology F: Foreign Terrorist Fighter (FTF) Typology

(Cases Nos. 2, 4, 5, 11, 25, 43 - Consolidated)

Several individuals have travelled to, or have attempted to travel to Syria, to join ISIL as Foreign Terrorist Fighters (FTF). They each have different recruitment stories and different means by which their travel to Syria has been facilitated.

Individual A was a student studying at University abroad and was radicalised and recruited by another student. Upon his return home, Individual A received funds via Western Union, from the student who recruited him. He uses those funds to purchase an airline ticket to Turkey, in order to join ISIL in Syria. He intends to meet up with his recruiter in Syria.

Individual B is one of 16 recipients located in 6 different countries to receive funding from 4 unrelated individuals in a foreign country. The funds were received in numerous remittances through a money remittance service. He uses these funds to facilitate his travel to Syria to join ISIL.

Individual C has successively changed his identity information, using different hotels in tourist areas as his personal addresses. He was nonetheless able to receive money transfers in each of three different identities on different occasions. All the money transfers are received from 3 persons located in another part of the country. Individual C is not related to these 3 persons, but the 3 persons are family members. In order to remit these funds to Individual C, these 3 family members have themselves received numerous cash transfers from several other unrelated persons.

Individual D is self-financing, using funds from his own bank account to fund his travel abroad. However, after he travels to the conflict area his account becomes silent for prolonged periods. If his debit card is used, it is for occasional purchases at stores near to an airport. However, while he is away, his credit card has been used within his home country, as if to give the impression that he has not travelled to a foreign country.

The FTFs have been recruited by individuals in various countries. Recruitment is done through social media, and in some cases through person-to-person contact and group meetings. Some of the FTFs also receive further additional financial and material support from recruiters while in transit to Syria. These various recruiters have received funding for their recruitment activities in various ways, namely:

- Use of their own legitimate income, proceeds from their criminal activities or unemployment benefits from the State;
- Receipt of funds in numerous small increments through money transfer services – from unknown individuals in various countries. In some cases, more significant funds have been received from some leaders of ISIL;
- Receipt from numerous persons of large numbers of wire transfers into their bank accounts in their home countries, whereupon funds are withdrawn in cash using debit cards in a country near the conflict zone, from which they are operating their recruitment and facilitation activities
- Receipt by wire transfer from one individual of the consolidated proceeds of wires transfers which they have received from numerous other unrelated individuals. Upon receipt of these funds, several airline tickets and travel and medical insurance are purchased, even though there is no evidence that the purchaser has travelled abroad.

Back to Table of Contents

Typology G: Changes in the economic profile of a customer

(Case No. 1)

An individual requested the financial institution to terminate his interest-bearing accounts, without giving explanation. The full content of deposit accounts was withdrawn in cash.

The teller reported that this individual refused to interact with any female employee of the bank and seemed to have changed his clothing and physical appearance, which might indicate some adherence to radical notions. A long period of silence was then observed on this account.

Source: France

Typology H: Use of Bitcoin to pay for webhosting

(Case No. 23)

Open source research identified an ISIL propaganda website used to solicit donations via bitcoin. Research into the bitcoin addresses identified five donations to the bitcoin addresses. The beneficiaries, in turn, made 12 payments for technical services or website hosting, including to the company that hosted the ISIL propaganda website. Bitcoin technology prevented the identification of the owner of the bitcoin addresses.

Source: Egmont ISIL Phase II project

Typology I: Use of IT specialists by terrorist organisations

(Case No. 26)

In 2012, a terrorist network recruited an IT specialist through the internet to support terrorist activities. He was arrested for engaging as an IT expert, assisting his partners, breaking into online-based MLM (Multi-Level-Marking)/investment. As a result of the hacking activity, the terrorist organisation managed to obtain some funds.

To receive and transfer the funds, the IT specialist used his wife's bank account, borrowed his relative's bank accounts, opened a new account with false identity, and bought other people's accounts with the intention to avoid tracing of funds. He also kept the value of the transaction in small amounts to avoid suspicion by the bank officials. From the account, several cash transactions were then carried out in favour of members of the terrorist network.

In the end, the IT specialist was convicted for terrorist involvement by financially supporting a terrorist organisation in Indonesia, utilising hacking techniques and conducting a meeting with several persons to raise donations for military training purposes in Poso (one of the conflict area in Indonesia), supporting violent extremists and their widows, and preparing future terrorist action.

Source: Indonesia

Back to Table of Contents

Typology J: Non-Profit Organisation and potential case of trade-based terrorist financing

(Case No. 38)

This case was initiated by an STR submitted by a bank to the Niger FIU. Cash was deposited into the account held by an NPO, then immediately transferred or withdrawn. The subsequent investigation revealed the NPO received USD 6 million in illicit transactions over a two year period from two affiliated religious associations based in Europe. The two main directors of the NPO were originally from a country in the Middle East and the NPO listed well-drilling (for water) and general trade as its main activities. A number of information exchanges between FIUs (including three European FIUs) revealed that the head of one of the religious associations had previously been accused of tax evasion and donation fraud. That same religious association had also been registered on the list of 'dangerous movements' in a European country. To facilitate the illicit transactions, the directors of the NPO created a shell Import-Export company in Niger. The Import-Export company director was European, but had originated from the same country as the directors. More than 80 per cent of the funds received by the NPO were transferred to accounts belonging to the shell company, as payment for services provided. However, information received from customs revealed the company had never imported/exported anything, despite numerous financial transactions received from neighbouring countries.

Investigations are ongoing.

Source: Niger

Typology K: Terrorist Proclivities of Foreign Work Permit-Holder

(Case No. 59)

Summary of Activity: A Bulgarian national (Suspect A) was arrested during an attempt to travel with another Bulgarian national (Suspect B), who had recently ceased employment in Country A, to Country B by boat. They were transporting a large load of used items found at a local waste facility, especially copper coils that had been removed from discarded air conditioners. Both of the Suspects were arrested but not convicted of terrorist offenses and were subsequently released and deported to Bulgaria as no links to designated terrorist organizations or designated terrorists could be established. Upon their release, local law enforcement shared the intelligence with their overseas competent authorities. Upon the Suspects' arrival in Bulgaria, Bulgarian authorities raided the residence of the Suspects, foiling a potential terrorist attack using explosives and seizing evidence of other associated radical persons. As a result of Country A's sharing of intelligence, it was later identified via STRs filed by banks and MSBs under ML (not TF) that the Suspects had continued to receive funds from persons in Country A.

Due to Country A's reputation of being a wasteful nation, the Suspects took advantage of the used supplies at the waste facility, acquiring copper parts that could be used to make explosives. According to Open Source information, bombs can be made from molten copper as the copper can be turned into a concave cone to seal an explosive charge in an improvised explosive device. When the explosive is detonated by, for example, a mobile phone trigger, the copper transforms into a forceful jet-stream of molten metal known as a plasma. This plasma jet easily perforates ordinary steel armour, hitting the surface at a speed of 8,000 meters per second and extremely high pressure. (https://Onceuponaparadigm.wordpress.com/2011/06/24/attacking-a-convoy-with-a-bomb-of-molten-copper/)

Back to Table of Contents

Financial Analysis: There was extensive SAR reporting after the public reporting of efforts by law enforcement to foil the attacks, mainly by banks and MSBs. The financial transactions included:

- Purchase of fuel for the boat whilst in the Caribbean and South America
- Purchase of airline tickets to Bulgaria
- Purchase of groceries (everyday expenses)
- An abnormally high number of EFTs sent by Country A residents to Bulgaria, and neighbouring countries, Turkey and Greece, via MSBs

Data Overview

Type or terrorism: Terrorist resourcing

Used means: None

Targets: None

Statement: None

Claimed: No

Connections: Close contact of a number of radical persons

Financial products: Use of debit and credit cards that had yet to be closed once expatriate Suspect's work permit had been terminated

STR/SAR reporting: Extensive reporting also on TF indicators by local banks and MSBs after the attacks

Possible Financial indicators:

- An abnormally high number of EFTs sent by Country A residents to Bulgaria, and neighbouring countries, Turkey and Greece, via MSBs

Source: Bulgaria

Typology L: Potential misuse of an NPO to engage in recruitment activities and misuse of donations

(Case No. 15)

A French NPO had the official aim of teaching the practice of religion. The NPO piloted a project aiming to acquire a new facility, to convert into a cultural centre at the cost of EUR 1.5 million. Voluntary contributions from followers and corporate donors provided the funding.

French authorities are still conducting their financial investigations and there has been no formal evidence of the use of funds for recruiting purposes. However, the religious leader behind the project has a lengthy criminal history and is known for his close links with a religious fundamentalist movement. As a religious leader, he is suspected of having significantly influenced the recruitment and departure of several young people to the Syrian-Iraqi zone. Further intelligence, which could not be revealed for the purposes of this report, suggests links between the founder/s and activities to recruit individuals to join terrorist organisations.

Financial flows on the NPO's bank accounts have revealed that the religious leader used the NPO's funds to pay his lawyer's fees (he is currently under house arrest) and organised crowd-funding operations dedicated to support his personal defence.

Source: France

Back to Table of Contents

Appendix E: List of Tables

List of Tables

APPENDIX F

BERMUDA - DIGITAL ASSET BUSINESS RISK ASSESSMENT REPORT

GOVERNMENT OF BERMUDA
Ministry of Finance

NATIONAL ANTI-MONEY LAUNDERING COMMITTEE
December 2024

BERMUDA - DIGITAL ASSET BUSINESS RISK ASSESSMENT REPORT

GOVERNMENT OF BERMUDA
Ministry of Finance

NATIONAL ANTI-MONEY LAUNDERING COMMITTEE
December 2024

Back to Table of Contents

Table of Contents

Back to Table of Contents

Executive Summary

The 2023 Digital Asset Business Risk Assessment (2023 Risk Assessment) was a thematic assessment of the Money Laundering (ML) threats and vulnerabilities affecting the licensed Digital Asset Business (DAB) sector in Bermuda, as well as the threats associated with the use of or exposure to digital assets in Bermuda.

During the original policy development and drafting stage of the Digital Asset Business Act 2018 (the Act), the Bermuda Monetary Authority (Authority or BMA) assessed the ML and Terrorist Financing (TF) risks associated with the DAB sector. The assessment was based on global developments and also considered the nature of the licences under consideration for inclusion in the draft legislation. Although the DAB sector was in Bermuda's 2020 Terrorist Financing National Risk Assessment, this is the first time ML risks in this sector is being assessed since the Digital Asset Business Act 2018 was enacted.

While this 2023 Risk Assessment was a sectoral assessment, the Working Group (WG) also considered the broader national threats and vulnerabilities related to the uptake of digital assets in Bermuda. This aspect of the risk assessment was more detailed. It recognises that anyone in Bermuda can access, store and spend digital assets using the services of Virtual Asset Service Providers (VASPs) located anywhere outside Bermuda. Therefore, local DAB-related ML threats may not solely originate within Bermuda's licensed DAB sector. The ability of competent local authorities to combat such threats also needed to be considered.

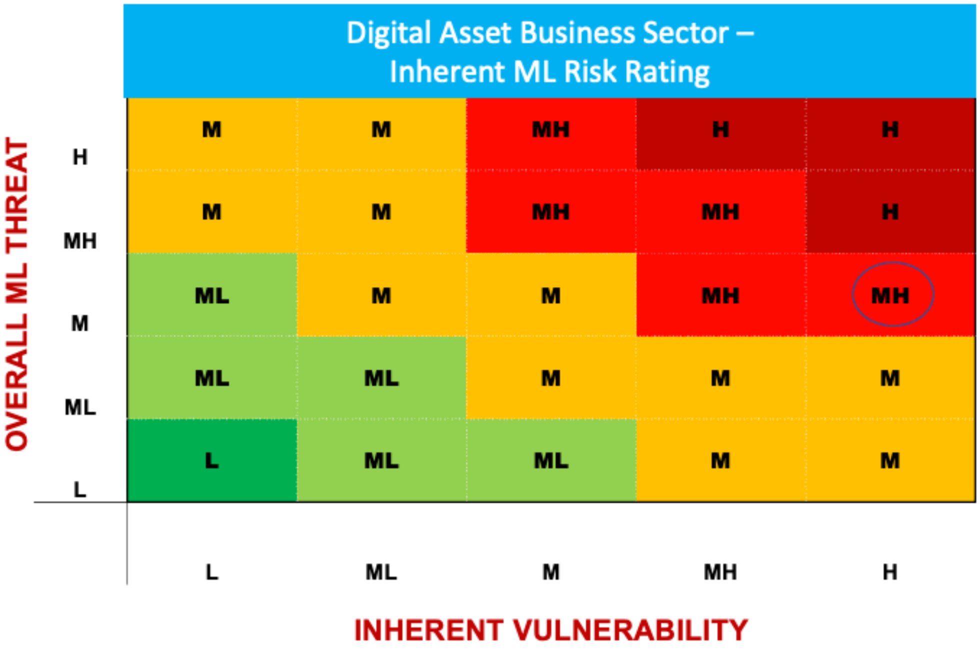
Based on this assessment, the ML threat rating to the DAB sector in Bermuda was determined to be MEDIUM. Bermuda's ML threat profile regarding digital assets is primarily associated with the suspected laundering of foreign proceeds of crime, particularly those related to fraud. All previous National Risk Assessments (NRAs) acknowledge that foreign ML threats are predominant in Bermuda. It is, therefore, logical that the foreign threats would have a more significant impact on Bermuda's overall ML risk related to digital assets. The assessment also demonstrates there is a lack of evidence that Bermuda's DAB sector was involved in any material level of ML activity. It is suspected that a relatively low amount of domestic criminal proceeds, primarily from drug trafficking, are being laundered through foreign DABs that do not directly operate in Bermuda.

Analysing sectoral vulnerabilities determined that the DAB sector's inherent vulnerability to ML was HIGH and consistent with the global picture. Internationally, VASPs have a HIGH exposure to lawbreakers' misuse, which makes many of the products and services offered by DABs attractive. Although this finding is broadly based on the global experience, the 2023 Risk Assessment did not examine the inherent vulnerabilities of the sector at the individual product and service level. Therefore, during the upcoming NRA update scheduled for 2024, the DAB sector will be assessed again using more recent data and the new World Bank risk assessment model for VASPs. This World Bank model is designed to address inherent vulnerabilities based on the products and services offered in the sector.

Back to Table of Contents

Given the findings on the ML threats affecting the licensed DAB sector, the sector's inherent ML risk rating is MEDIUM-HIGH, as shown in the Heat Map below.

Figure 1: Risk Heat Map – Digital Asset Business Sector - Inherent ML Risk Rating



Digital Asset Business Sector –
Inherent ML Risk Rating

OVERALL ML THREAT

H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

INHERENT VULNERABILITY

Mitigating measures for DABs are fully aligned with those for all other financial sectors. The BMA's holistic approach to regulation of the DAB sector incorporates both prudential and AML obligations. This approach replicates all of the key components of risk assessment, licensing, regulation and guidance, offsite and onsite supervision, enforcement, and monitoring and reporting that characterise the regulation of all other financial sectors under the BMA's ambit.

This risk assessment also examined the effectiveness of the Act's framework and the oversight mechanisms implemented nationally and within the sector to mitigate risk. The 2023 risk assessment also leveraged the work done in the 2020 ML NRA. As with all previous risk assessments, it continued the tradition of identifying areas for continued development, as enhancement of the AML/ATF regime remains a core objective of the National Anti-Money Laundering Committee (NAMLC).

Back to Table of Contents

Introduction

In accordance with the National Anti-ML (AML)/Anti-TF (ATF)/Counter-Proliferation Financing (CPF) Policy, NAMLC is responsible for ensuring that competent authorities collaborate to keep Bermuda's understanding of its ML risk up to date and for developing and proposing to Cabinet any policies or strategies with a focus toward mitigating the identified risks. In this context, NAMLC conducted the ML National Risk Assessment (ML NRA) from 2020 to 2021. However, including the DAB sector in the evaluation was not feasible at that time. Nonetheless, NAMLC strived to ensure that a specialised assessment of that sector would be conducted in the future within a reasonable timeframe. In addition, a report on the findings would be appended to the previously published 2020 report on the ML and TF NRA's outcome.[1] Following this, in 2023, NAMLC conducted Bermuda's first Digital Asset Business Risk Assessment and remains committed to finalising the resulting report promptly for inclusion in the 2020 ML NRA.

The approach to this assessment was to have a focused WG assess the ML risks involving digital assets in Bermuda. The WG included NAMLC members from the BMA, Attorney General's Chambers (AGC), Bermuda Police Service (BPS), Department of Public Prosecution (DPP), Financial Intelligence Agency (FIA) and Office of NAMLC. Simultaneously, the BMA also assessed the inherent vulnerabilities in the sector and the effectiveness of the AML/ATF controls applied to and in this sector.

The methodology used to carry out this assessment was customised, given the Bermuda context and the fact that it would be the first assessment for the DAB sector. The methodology is, therefore, comprised of the following three components for assessment;

1. ML threats affecting the DAB sector and related to digital assets;
2. Bermuda's ability to combat ML related to DABs or involving digital assets; and
3. Inherent sectoral vulnerabilities and controls.

This report on the NRA focuses solely on the findings concerning components one and three, namely the assessment of ML threats affecting the DAB sector and related to digital assets and the assessment of inherent sectoral vulnerabilities and controls in the DAB sector. Bermuda’s AML/ATF Legislative Framework and key agencies can be found at Chapter 2 of the Report and Bermuda’s AML/ATF Operational Framework can be found at Chapter 3 Of particular relevance to this sectoral assessment is the description of the Bermuda Monetary Authority’s Supervisory Framework, commencing on page 23, given that this framework is applied to Digital Asset Businesses as they are regulated by the BMA.

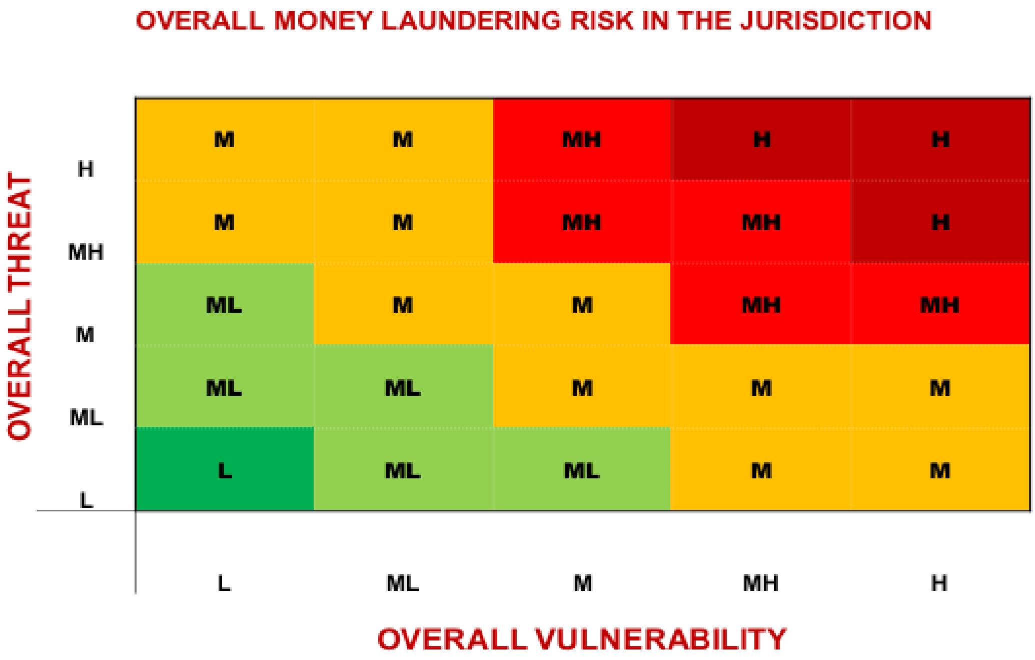
Finally, the World Bank’s ML NRA model provides a matrix in the form of a heat map (see Figure 2: Risk Hat Map – Threats and Vulnerabilities Matrix) to combine the rankings of National ML Threats and National ML Vulnerabilities (combatting ability) to generate an overall ML risk for Bermuda. This same matrix can be used to create the overall and/or inherent sectoral risk ratings, using the vulnerability rankings generated in the sectoral vulnerability assessment and the sectoral threat rankings generated during the assessment of ML threats.

[1] See published report on the outcome of the 2020 ML and TF Risk Assessments: www.gov.bm/sites/default/files/2020-Money-Laundering-Terrorist-Financing-Risk-Assessments.pdf

Back to Table of Contents

Figure 2 illustrates the threat/vulnerabilities matrix. The risk levels have been colour-coded, with lower levels depicted in shades of green, medium levels in yellow, and higher levels in red.

Figure 2: Risk Heat Map - Threats and Vulnerabilities Matrix



OVERALL MONEY LAUNDERING RISK IN THE JURISDICTION

OVERALL THREAT					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

OVERALL VULNERABILITY

Back to Table of Contents

Chapter 1: Money Laundering Threat Profile

Summary of Findings:

Final Threat Rating – MEDIUM - Bermuda's ML Threat Profile for digital assets is primarily driven by the laundering of foreign proceeds of crime particularly related to fraud. Some local proceeds are suspected of being laundered through DABs including those related to drug trafficking.

1. Introduction

Bermuda has undertaken an ML Sectoral Risk Assessment for DABs as part of its ongoing effort to understand the ML risks present in the jurisdiction. The risk assessment was executed using a methodology created by the World Bank's Virtual Asset Risk Assessment Module. In addition, an assessment of national threats and vulnerabilities was conducted specifically concerning digital assets, based on the World Bank's ML NRA tool. This section of the report provides an overview of the ML threats for DABs and the use of digital assets.

2. Process and Scope

The WG leveraged the findings from the ML threat assessment completed in the 2020 NRA. The WG accepted the accuracy and continued relevance of the findings that were outside the scope of digital assets and the DAB sector. The purpose of this report is to focus solely on threat factors relevant to the DAB sector and digital assets. The WG was comprised of representatives from competent authorities responsible for law enforcement, prosecutions, financial intelligence and national coordination.

Similar to the National ML Threat Assessment, the assessment examined four aspects, which consisted of the following:

1. Predicate Offence Breakdown – relevant predicate offences that generate proceeds and give rise to ML in the DAB sector or using digital assets;
2. Origins Breakdown – origins of the ML threats;
3. Sector Breakdown – analysis of the sectoral threats for the licensed DAB sector; and
4. Overall ML threat assessment.

The Predicate Offence Breakdown collects and analyses statistics and information regarding crimes and ML cases involving digital asset businesses within the jurisdiction that generate proceeds. The purpose of this analysis is (1) to help establish which type of predicate offence is most prevalent using or involving digital assets, whether or not a DAB in the jurisdiction was involved, and (2) to estimate the size of the proceeds generated by these crimes that have used digital asset businesses to launder the proceeds. The Predicate Offence Breakdown section also calls on the WG to estimate undetected and unrecorded predicate offences and their proceeds. The analysis focused on those predicate offences that were determined to be relevant based on the case data from the AGC, BPS, DPP and FIA.

Back to Table of Contents

The Origins Breakdown is designed to facilitate the identification of patterns regarding the originating jurisdiction of the proceeds of crimes. This may be particularly relevant in cases where the predicate offence to ML was committed in a foreign jurisdiction. There are four possible scenarios, as follows:

1. The predicate offence is committed in a foreign jurisdiction, but the proceeds are laundered in Bermuda;
2. The predicate offence is committed and the proceeds of crimes are laundered in Bermuda. Even if the proceeds are later transferred to other jurisdictions, some initial acts of the laundering offence have occurred in Bermuda;
3. The proceeds that are laundered in Bermuda are generated by predicate offences committed domestically and in foreign jurisdictions; and
4. The origin of the proceeds of crimes cannot be identified. Therefore, whether they are generated in Bermuda or foreign jurisdictions is unclear.

The Origins Breakdown analysis was based on case data collected from the FIA, BPS, DPP and AGC.

The Sector Breakdown section analyses the ML threat as it materialises within digital asset businesses in the jurisdiction. This section of the report analyses how the proceeds are invested and laundered in the DAB sector.

Upon completion of the tables, significant information was available that enabled the WG to complete the Overall ML Threat Analysis. Data collected on internal, external and sectoral threats was used. The analysis contains some cross-references to these parts of the assessment, which made it possible to develop an assessment of the overall threat. The result is the primary input to establishing the overall ML risk for the DAB sector.

3. Identified Crimes that Generate the Proceeds Laundered through Digital Asset Businesses

In conducting its threat analysis of crimes that generate proceeds laundered through digital asset businesses, the WG focused on 10 predicate offences. These were identified based on the intelligence and case-based data and include fraud (domestic and foreign), corruption (domestic and foreign), cybercrime, drug trafficking, distribution of child pornographic materials, murder for hire, terrorism financing and market abuse. The ML threat rating for these predicate offences can be found in Table 1.

Back to Table of Contents

Table 1: ML Threat Ranking of Predicate Offences

Threat Ranking of Predicate Offences	ML THREAT ASSESSMENT 2023
Fraud (foreign)	Medium
Fraud (domestic)	Low
Corruption (domestic)	Low
Corruption/bribery (foreign)	Low
Cybercrime	Low
Drug trafficking	Medium
Distribution of child pornographic materials	Low
Murder (conspiracy to murder)	Low
Terrorism financing	Low
Market abuse (e.g., insider trading)	Low
Organised crime (no similar offence in Bermuda)	Not rated in this assessment
Human trafficking (no similar offence in Bermuda)	Not rated in this assessment
Sexual exploitation	Not rated in this assessment
Arms trafficking	Not rated in this assessment
Trafficking in stolen goods	Not rated in this assessment
Counterfeiting of currency	Not rated in this assessment
Counterfeiting and piracy of products	Not rated in this assessment
Environmental crime	Not rated in this assessment
Kidnapping, illegal restraint, hostage-taking	Not rated in this assessment
Robbery/theft/stealing/taken without consent, etc.	Not rated in this assessment
Smuggling	Not rated in this assessment
Extortion	Not rated in this assessment
Forgery	Not rated in this assessment
Piracy	Not rated in this assessment
Insider trading and market manipulation	Not rated in this assessment
International Tax Evasion Investigations	Not rated in this assessment
Contributory Pension/Pension Fraud	Not rated in this assessment
Domestic Tax Evasion	Not rated in this assessment

None of the predicate offences were rated as High in this context, while eight were assessed as Low, and two, namely, foreign fraud and drug trafficking, were rated as MEDIUM threats.

Back to Table of Contents

a) **Foreign fraud was rated as a MEDIUM threat.** This is due to intelligence reporting that suggested the amount of ML related to foreign fraud has not been significant. The threat included using stolen Application Programming Interface (API) keys, identity theft and defrauding investors and other persons through scams by foreign fraudsters targeting victims internationally, including Bermudians. **Nonetheless, Bermuda is mindful of the stark increase in large-scale crypto-related frauds, that have occurred on a global scale,** especially in the US market, involving so-called "pump-and-dump" schemes involving NFTs and various coins, and other fake and fraudulent investment opportunities geared at using crypto hype to target investors. Globally, hundreds of millions of dollars have been lost to these schemes, with little knowledge as to where these funds have ended up.

b) **Drug trafficking was assessed as a MEDIUM threat2.** The BPS reports that the currency conversion and cash courier method is still primarily being used by Bermudian drug traffickers. However, the reports also indicated that 'seeds' have been found with some frequency during drug search operations. Seeds are the codes that individuals use to recover access to crypto wallets. These findings led to the conclusion that ML related to drug trafficking activity in Bermuda may now be occurring through the use of digital assets. However, the extent to which this method has replaced traditional cash couriers is unclear. Regardless of the method used to move drug trafficking proceeds out of Bermuda, the size of the laundered proceeds will be limited to the size of Bermuda's relatively small illicit drug market.

c) **Domestic fraud was assessed as a LOW threat and no domestic fraud using DABs was recorded.** Nonetheless, analytical tools identified suspects with Bermuda IP addresses who have received cryptocurrencies via foreign-based DABs suspected to have originated from fraud.

d) **Corruption (domestic) and corruption and bribery (foreign) were assessed as LOW threats.** There are no suspected domestic or foreign ML cases connected to DABs.

e) **Cybercrime was assessed as a LOW threat**. Information regarding abuse of the elderly and identified thefts conducted by hacking cryptocurrency accounts and stealing API keys was received; however, no transactional activity was noted. International cooperation identified the sale of ransomware using dark markets where parties were invited to purchase malicious software using cryptocurrencies. The foreign Law Enforcement Agency (LEA) determined that suspects had accounts with Bermudian DABs, and the information requested by the foreign LEA on the Bermudian DABs was sent.

[2] In Bermuda's 2020 ML NRA, drug trafficking was rated as a High threat for ML.

Back to Table of Contents

f) **Distribution of child pornographic materials was assessed as a LOW threat**. Investigations are ongoing in the transfer of digital assets from a Bermuda resident to a person in Indonesia who is known to source and distribute child pornography. This single case is under current investigation but has not given rise to the view that ML from this crime is a pervasive issue in Bermuda. There is no reason to believe that any material level of the ML arising from this offence has occurred in Bermuda or that such activity is utilising a DAB for the purpose of ML in Bermuda.

g) **Conspiracy to murder was assessed as a LOW threat.** There is one case of domestic murder-for-hire under investigation involving a Bermuda resident where digital assets were used as payment. This crime was committed in 2017, although was first detected by BPS in 2022. The payment was made in Bitcoin. The investigation into the conspiracy to murder is ongoing in Bermuda, although ML is not part of the investigation. The foreign country/ countries to which the Bitcoin payment was sent may be considering ML charges connected to the Mutual Legal Assistance requests related to this offence. Payment in Bitcoin at the time was the equivalent of USD $5,268 (12 bitcoins). The value of Bitcoin was under USD $450 at the time of the transaction but has skyrocketed since. As the case is still pending, decisions on potential seizure will be made at the conclusion of any court proceedings. . BPS is of the view that ML from murder-for-hire schemes is not occurring using Bermudian DABs. It should be noted that the website used in this offence to pay for such offences using cryptocurrency was available to anyone globally. The site has been taken down, but copycat dark websites have been created.

h) **Terrorism was assessed as a LOW threat.** No intelligence, information or cases exist connected to suspected ML arising from TF occurring in Bermuda.

i) **Terrorism financing is a LOW risk in Bermuda based on Bermuda's 2020 TF NRA.** The limited number of reports received by the FIA has not challenged that finding or provided any evidence that ML arising from TF is occurring in Bermuda using digital assets.

j) **Market abuse (Insider Trading) was assessed as a LOW threat**. There are no suspected cases of ML involving local or overseas with connections to DABs.

k) **Other predicates**: No intelligence or investigation was initiated regarding ML involving digital assets or DABs related to any other predicate offences. The assessment aimed to identify and assess the predicate offences relevant to the misuse of digital assets or DABs for ML purposes in Bermuda, and therefore, the WG only assessed the predicate offences identified as relevant by the data.

Back to Table of Contents

4. Origin of Proceeds of Crime

Some criminal proceeds generated in Bermuda are being laundered using digital assets. As highlighted previously, BPS intelligence believes that criminals may be laundering drug trafficking proceeds using digital assets, although no specific case has been detected. The size of the laundered proceeds related to drug trafficking will be limited to Bermuda's relatively small drug market. Furthermore, the case of murder-for-hire originating in Bermuda, as previously mentioned, used a foreign DAB for the remitting of payment.

The ML threat originating from offences committed in Bermuda and involving DABs is assessed as MEDIUM.

Fraud is the primary predicate offence where the offence is committed in foreign jurisdictions and the proceeds are suspected to be subsequently laundered through Bermuda DABs. The FIA has received 93 suspicious filings where a Bermuda DAB was possibly being used to launder funds related to foreign fraud. The BPS has also conducted investigations at the request of foreign LEAs related to fraud conducted internationally. Additionally, one investigation was triggered by intelligence from a foreign Financial Intelligence Unit (FIU) that indicated that a resident guest worker accessed child pornography from a network of individuals in Indonesia who were under investigation there for the distribution of such materials. While this Bermuda resident used digital assets to remit payment to obtain the pornography, this was done through a foreign DAB.

The ML threat originating from offences committed in foreign jurisdictions and involving Bermudian DABs is assessed as MEDIUM.

The value of transactions related to predicate crimes committed in Bermuda and a foreign jurisdiction where the criminal proceeds are laundered through DABs in Bermuda is considered LOW. The types of cases included in this category include internet scams, where foreign offenders target domestic victims to send money or cryptocurrency through various financial channels. However, the value of the transactions involved in the majority of these cases is relatively low, and it is also often difficult for law enforcement to determine whether a local DAB was used in these circumstances. Therefore, no material ML is believed to occur in local DABs, where domestic and foreign predicate offences give rise to the proceeds.

The ML threat originating from offences committed both domestically and in foreign jurisdictions that involve Bermudian DABs is assessed as LOW.

Based on the findings of this assessment, there are currently no ML threats with unidentifiable origins. Therefore, the ML threat related to the unknown origin is assessed as LOW.

In summary, foreign ML threats predominate in Bermuda, including funds laundered through the domestic DAB sector. The level of domestic proceeds laundered, particularly related to drug trafficking, cannot yet be fully ascertained.

Back to Table of Contents

Table 2: Origin Breakdown 2020-2022

	Origin of Laundered process	Number of ML cases investigated	Number of ML cases prosecuted	Number of ML convictions (cases)	Number of persons Convicted on ML	Amount of ML proceeds seized or frozen on ML	Amount of ML proceeds confiscated	ML Threat
A	Offences committed in home jurisdiction	2	0	0	0	0	0	MEDIUM
B	Offences committed in a foreign jurisdiction	2	0	0	0	0	0	MEDIUM
C	Offences committed both in home and foreign jurisdiction	0	0	0	0	0	0	LOW
D	Origin country cannot be identified	0	0	0	0	0	0	LOW
	TOTAL	4	0	0	0	0	0	

5. Sector Breakdown

During the assessment period, the FIA received 366 Suspicious Activity Reports from the DAB sector. Per information provided by the largest single filer, the majority of their suspicious activity reports were also filed with an FIU overseas, due to their licencing/registration obligations.

Based on the SARs received, a number of ML indicators can be derived:

- Attempted unauthorised transfer and unauthorised access
- Doctored identity documents
- Fraudulently accessed trading API keys (account takeover)
- An account that has been compromised with unauthorised outgoing transfers
- Adverse media identified
- Attempted use of multiple accounts to obscure the ultimate source of funds and the nature of these accounts
- Concerns about source of wealth or source of funds direct exposure to person-to-person (P2P) exchange

Back to Table of Contents

- Credit card fraud
- Customer has a non-compliant business partner
- Exposure to a gambling service
- Exposure to a Ponzi scheme link
- Exposure to an address linked to illicit drug sales
- Exposure to an exchange with a potential link to Iran
- Exposure to forex and cryptocurrency investment schemes alleged to be scams
- Exposure to ransomware
- Exposure to a suspected child abuse/paedophilia address
- Failure to provide onboarding documents
- Identity theft
- Direct or indirect exposure to mixing service
- Exposure to P2P exchange (localbitcoin.com)
- Indirect exposure to a scam
- Indirect exposure to illicit actor organisation
- Indirect receiving exposure from a fraud shop
- Detection of chain peels from different exchanges and P2P exchanges
- Direct exposure from high-risk jurisdiction (Iran)
- Direct exposure to an identity theft ring
- Direct exposure to high-risk exchange
- Direct receiving exposure from sanctioned addresses
- Exposure to coin swap service
- Indirect exposure to loan laundering
- Involved in market manipulation and wash trading

To further explain the indicators outlined above, direct exposure represents services or other entities that are direct counterparties of the target address across any of its transactions. Indirect exposure measures the services and entities that make up the origins or destinations of funds in the target address transactions in cases where non-service addresses exist between the target address and those services or entities.

Back to Table of Contents

The sectoral threat level is assessed to be MEDIUM. The FIA has received 366 SARs from the DAB sector. The majority of these involve predicate offences committed internationally. When coupled with intelligence indicating a medium threat of domestic predicates, primarily drug trafficking, the overall sectoral threat rating was assessed to be MEDIUM.

6. Risk Assessment Findings

In assessing the ML threat that exists in the DAB sector based on the relevant data and information, the following findings were made:

- Foreign fraudsters involved in the laundering of proceeds of foreign fraud are targeting Bermuda DABs at a moderate level
- Foreign DABs are believed to be involved in laundering proceeds from domestic drug trafficking
- DABs are involved in the laundering of domestic fraud, corruption, cybercrime, distribution of child pornographic materials, murder (for hire), terrorism financing and market abuse at a low level
- Four ML investigations involving foreign and domestic DABs were launched during the assessment period. Two were related to offences committed domestically and two were related to offences committed in foreign jurisdictions
- SAR data indicate that the majority of filings are related to suspicions of predicate criminal offences committed internationally with individuals with no ties to Bermuda

Based on the above findings, the Bermuda DAB ML threat level is assessed to be MEDIUM. Foreign ML threats predominate in Bermuda's DAB sector. This is in keeping with a similar finding in all previous NRAs when evaluating threats. Therefore, the ML threat from foreign predicate offences is anticipated to significantly impact Bermuda's overall ML threat more than domestic offences involving digital assets.

7. Concerns or Challenges with the Threat Assessment

For this initial DAB sectoral threat assessment, there were no particular concerns or challenges identified. It was noted that SARs reported to the FIA were primarily related to suspicions of predicate criminal activity outside of Bermuda, highlighting the importance of international co-operation by the FIA.

Back to Table of Contents

Chapter 2: DAB Sectoral Vulnerabilities

Summary of Findings:
The inherent vulnerability of the DAB sector was determined to be HIGH, with a MEDIUM rating for ML threats specfically.

1. Introduction

The DAB Sector was launched in 2018. It has been within the scope of AML/ATF regulation under the Proceeds of Crime Act (POCA) 1997 from its inception and has been supervised by the BMA. As of the end of 2022, the sector comprised eight Class F licences, four Class M licences and four Class T licences. The Authority continues to receive DAB licence applications, which may include applications from businesses with complex business models or those that span other licensed sectors and require collaboration and joint supervisory efforts across various prudential supervision teams within the BMA.

2. Methodology and Scope

The methodology and scope for this analysis were tightly focused. In line with our standard approach towards all initial NRAs for new or emerging financial sectors, this initial assessment of the DAB sector focused on an industry-wide evaluation of inherent vulnerabilities. To analyse these inherent sectoral vulnerabilities, the WG conducted a comprehensive assessment utilising the same World Bank approach and methodology historically used to assess other financial sectors. The WG reviewed the World Bank's specific sectoral assessment methodology for Virtual Assets and VASPs and decided to adopt it for future assessments. The scope of the assessment included DAB entities that were conducting duly licensed business during the assessment period.

3. Analysis of Sectoral Inherent ML Vulnerabilities

The inherent vulnerability rating of the DAB sector was determined to be HIGH due to the factors detailed below.

- The total number of licensees in the DAB sector is low compared to the other more traditional sectors. Only eight licensed entities existed during the assessment period

- The sector's client base profile was assessed to have HIGH vulnerability due to its international nature, the non-face-to-face nature of onboarding and transaction activity, and the internet-based nature of DAB activities

The level of cash activity is assessed as MEDIUM. Since this assessment was conducted using the traditional World Bank NRA sectoral assessment tool, capturing the cash activity within DABs proved challenging as cash is only held in digital form. This differs from traditionally obligated entities such as financial institutions and Designated Non-Financial Businesses and Professions. DABs convert fiat to Virtual Assets or vice versa via virtual asset exchanges rather than cash. Also, it should be noted that the VA transactional level activity is not captured by the tool used for this assessment, nor is it factored into the 'cash activity' assessment criterion. This accounts for the allocation of a rating of Medium in this instance.

Back to Table of Contents

The frequency of international transactions is rated as HIGH, given that all clients are global. Further, digital assets, by their very nature, are not constrained by any geographical borders. Although blockchain technology is essentially 'borderless', it does provide transparency and traceability of transactions. Implementing the travel rule can facilitate the tracing of transaction records.

A complete product risk assessment will be conducted in 2024 using the World Bank's bespoke tool for assessing VA/VASPs risks.

4. Mitigating Measures

Mitigating measures at the framework level for DABs are robust, and fully aligned with those for all other financial sectors. With the introduction of the Act, the BMA intentionally positioned the DAB sector to be regulated in the same manner and approach as the traditional financial sectors already under its ambit. The framework therefore includes ongoing risk assessment, licensing, regulation and guidance, offsite and onsite supervision, enforcement, and monitoring and reporting that characterise the regulation of all other financial sectors.

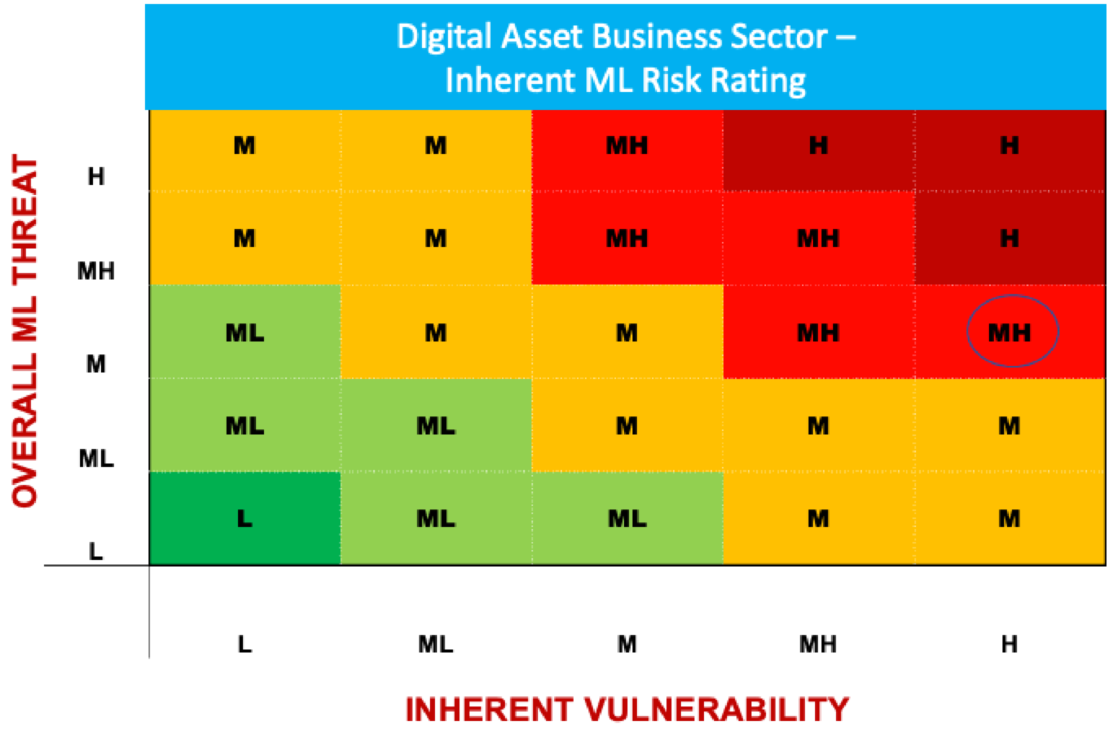
Of key importance to the framework is the definition of “digital asset” within the Act, to ensure as broad a coverage of possible of business activities in this rapidly evolving sector.

Conclusion

As the heatmap below indicates, the MEDIUM-HIGH ML inherent risk rating results from a High inherent vulnerability rating and a Medium rating for ML threat. While the inherent vulnerability assessment provided valuable insights, these insights are expected to broaden and deepen the next assessment using the complete World Bank VA and VASPs NRA tools.

Back to Table of Contents

Figure 1: Risk Heat Map – Digital Asset Business Sector – Inherent ML Risk Rating



	L	ML	M	MH	H
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	[✓ MH]
ML	ML	ML	M	M	M
L	L	ML	ML	M	M

This report is focused solely on inherent vulnerabilities. It is important to consider these in the context of the robust regulatory framework that has been established for the DAB sector. Ensuring that DABs continue to meet their obligations under this framework remains a key focus of the BMA. The complete assessment exercise brought attention to the following mitigation-related focal points for the DAB sector:

1. The importance of staff knowledge, as this is crucial to mitigate any risks arising from the sector's continued growth; and

2. The sector should ensure that its compliance and reporting systems are continuously updated and effectively implemented to ensure that they continuously meet their obligations in accordance with the AML/ATF legislation.

Back to Table of Contents

Appendix A: Glossary

AGC	Attorney-General's Chambers
AML	Anti-Money Laundering
API	Application Programming Interface
ATF	Anti-Terrorist Financing
BMA	Bermuda Monetary Authority
BPS	Bermuda Police Service
CPF	Counter Proliferation Financing
DAB(s)	Digital Asset Business(es)
DPP	Department of Public Prosecutions
FIA	Financial Intelligence Agency
FIU	Financial Intelligence Unit
LEA	Law Enforcement Agency
ML	Money Laundering
ML NRA	ML National Risk Assessment
NAMLC	National Anti-Money Laundering Committee
NRA(s)	National Risk Assessment(s)
POCA	Proceeds of Crime Act 1997
SARs	Suspicious Activity Reports
TF	Terrorist Financing
TF NRA	TF National Risk Assessment
VASPs	Virtual Asset Service Providers
WG	Working Group

Back to Table of Contents

Appendix B: Lists of Tables and Figures

List of Tables

List of Figures