



Digital Asset Businesses (DAB)

Money Laundering (ML)/Terrorist Financing (TF) Risks, Vulnerabilities and Preventive Measures

Presented by: Anti-Money Laundering /Anti-Terrorist Financing
(AML/ATF) and the Financial Intelligence Agency



22 August 2024



Agenda

- | | | | |
|----|-------------------------------|----|------------------------------------------|
| 01 | Introduction of speakers | 05 | Preventive measures |
| 02 | Sector overview | 06 | Travel Rule |
| 03 | Understanding the ML/TF risks | 07 | Onsite Findings and Examination Process |
| 04 | Understanding BRA and CRA | 08 | FIA Statistics, Typologies and Reporting |
| | | 09 | Conclusion |

Digital Asset Sector Overview

- Digital asset hub
- Diverse activities
- Regulatory framework
- BMA oversight
- AML compliance
- Innovation and compliance balance

Overview of AML/ATF and Sanctions Legislation

- 1997 Proceeds of Crime Act
- 2004 Anti-Terrorism Financial and Other Measures Act
- 2008 Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act
- 2008 Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations
- Additionally, under Section 12(6)(c) of the Digital Asset Business Act 2018, an RFI is obligated to meet the Proceeds of Crime (AML and ATF) Regulations 2008
- 2003 International Sanctions Act*.



**this is separate to AML requirements*

Sectoral Risk - Overall, Threat and Vulnerability Scores – DAB

- Our existing National Risk Assessment (NRA), generated through the World Bank Model, is uniquely tailored to the traditional financial sector, providing focused and informed insights into sector-specific risks
- The DAB NRA, which used a blended traditional financial sector World Bank Model covering 2020-2022 is in the final approval stage by NAMLC and will be released in the near future.
- Recognising the importance of this growing sector and the importance of risk assessments, the Authority plans to execute a further enhanced NRA specifically for the DAB Sector. We aim to share the details in due course.



Key Risks and Vulnerabilities that DABs should consider

- Anonymity
- Cross-border transactions
- Regulatory arbitrage
- Peer-to-peer and rapid transactions
- Privacy and emerging technologies
- Market manipulation
- Integration of Decentralised Finance (DeFi)
- Integration with traditional financial systems
- Outsourcing of AML/ATF functions:
 - Lack of direct control
 - Compliance variability
 - Insufficient training
 - Third-party relationships
 - Dependency risks
- Reliance on third parties:
 - Compliance gaps and legal obstacles to information sharing
 - Dependency and operational risks



Understanding the Institutional ML/TF risks - Business Risk Assessment

Identify and assess inherent risks

Consider all relevant risk factors with regard to the Regulated Financial Institutions' (RFI) customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions in order to assign inherent risk ratings

Establish risk tolerance

Determine the level of risk the business is willing to accept

Establish risk mitigation measures

Develop and document proportionate and effective policies, procedures and controls in order to minimise and manage the risks that have been assessed



Monitor and review risks

Maintain up-to-date risk assessment information and risk ratings and regularly review, test and improve the policies, procedures and controls put in place

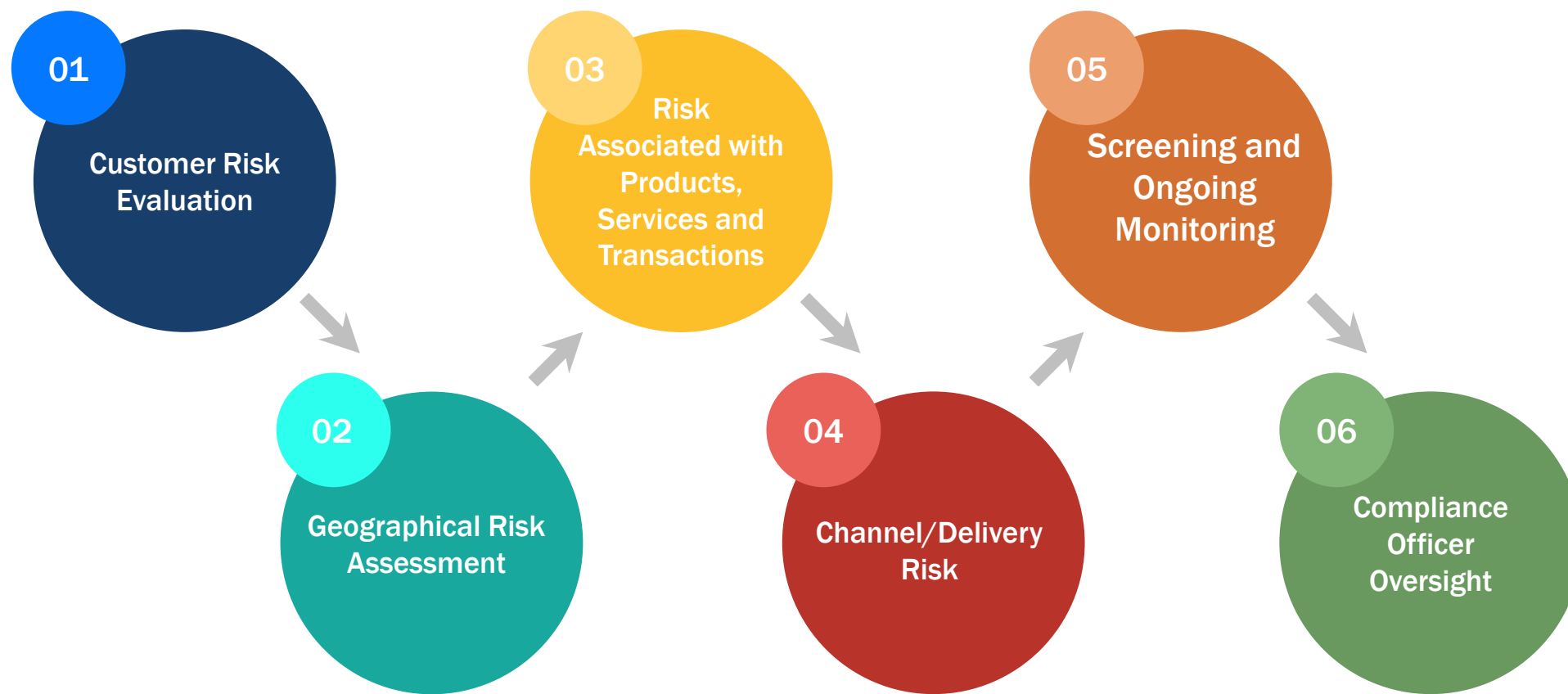
Implement risk mitigation measures

Apply the risk mitigation policies, procedures and controls that have been developed and documented

Evaluate residual risks

Determine the level of risk remaining after taking mitigation measures into consideration

Understanding the Institutional ML/TF risks - Customer Risk Assessment



Minimum requirement for assessing Customer Risk

DAB Sector - Preventive ML/TF measures

Customer Due Diligence (CDD):

- Verify identities
- Risk classification
- Ongoing monitoring

Transaction Monitoring:

- Detection systems
- Suspicious transaction reporting

Record Keeping:

- Documentation maintenance
- Comprehensive record-keeping



DAB Sector - Preventive ML/TF measures (Cont'd)

Risk-Based Approach:

- Tailored preventive measures
- Resource allocation

Employee Training and Awareness:

- Regular training
- Risk awareness

Reporting Obligations:

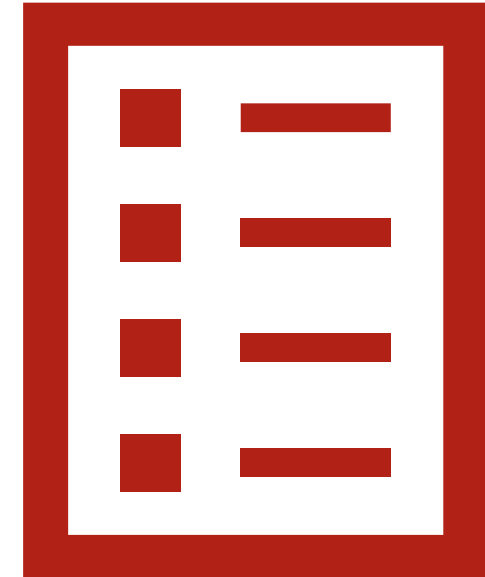
- SAR submission

Internal Controls and Policies:

- Effective controls
- Policy alignment
- Reliance & Outsourcing
- AML Independent Audit

Screening:

- Relevant sanctions lists
- Robust screening procedures



Travel Rule

Travel Rule Compliance	Payer/Originator Payment Service Provider				
	Informative elements that must <i>travel</i> with transaction	Payer		Payee	
	All DA Transfers	Verifies and transmits	<ul style="list-style-type: none">• Full name• Account number and address (if address not available, can be replaced with place and DOB, customer identification number or national identity number)	Transmits	<ul style="list-style-type: none">• Full name• Account number (if not available, must be replaced with unique identifier)
	DA Transfers to self-hosted wallets	Obtains and records		Obtains and records	
Measures applicable to transfers of digital assets					

Travel Rule (Cont'd)

Travel Rule Compliance Measures applicable to transfers of digital assets	Payee/Beneficiary Payment Service Provider				
	Informative elements that must <i>travel</i> with transaction	Payer		Payee	
	All DA Transfers	Detects	Mandatory informative elements on the Payer/Originator (slide above)	Detects and verifies	Mandatory informative elements on the Payee/Beneficiary (slide above)
	DA Transfers from self-hosted wallets	Obtains and records		Obtains and records	

Travel Rule (Cont'd)

Intermediary Payment Service Provider

All DA
Transfers

Detects,
transmits and
records

Mandatory informative
elements on the payer
and payee.
(slide above)

1. Implements effective procedures to:

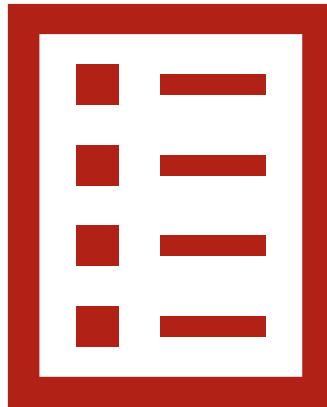
- Detect whether digital asset transfers are accompanied by information about the originator and the beneficiary
- Determines, based on risk assessment, whether to execute or reject a digital asset transfer without complete information about the originator or beneficiary

2. Report to the BMA if PSP regularly fails to supply the information on the payer.

3. Considers the omission and incompleteness of information as factors for applying enhanced measures and assessing suspicion of ML/TF and filing SARs with FIA.

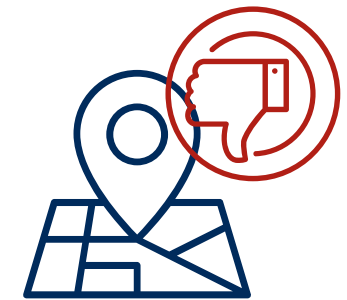
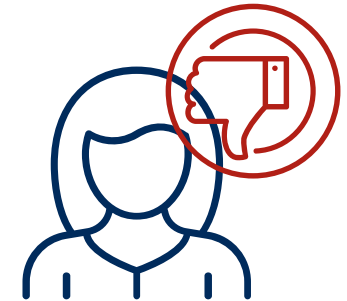
DAB Onsite/Offsite Non-compliance Trends

- Inadequate customer due diligence
- Lack of ongoing monitoring
- Customer ID and address verification – meeting the Bermuda standard requirement
- Inadequate BRA and CRA
- Use of ‘Shelf’ policies
- Inadequate Bermuda-specific training
- Lack of quality Independent ML/TF Audits
- Lack of remedial action regarding ML/TF independent audit findings
- Balancing Fiduciary responsibilities with AML/ATF Regulatory Compliance

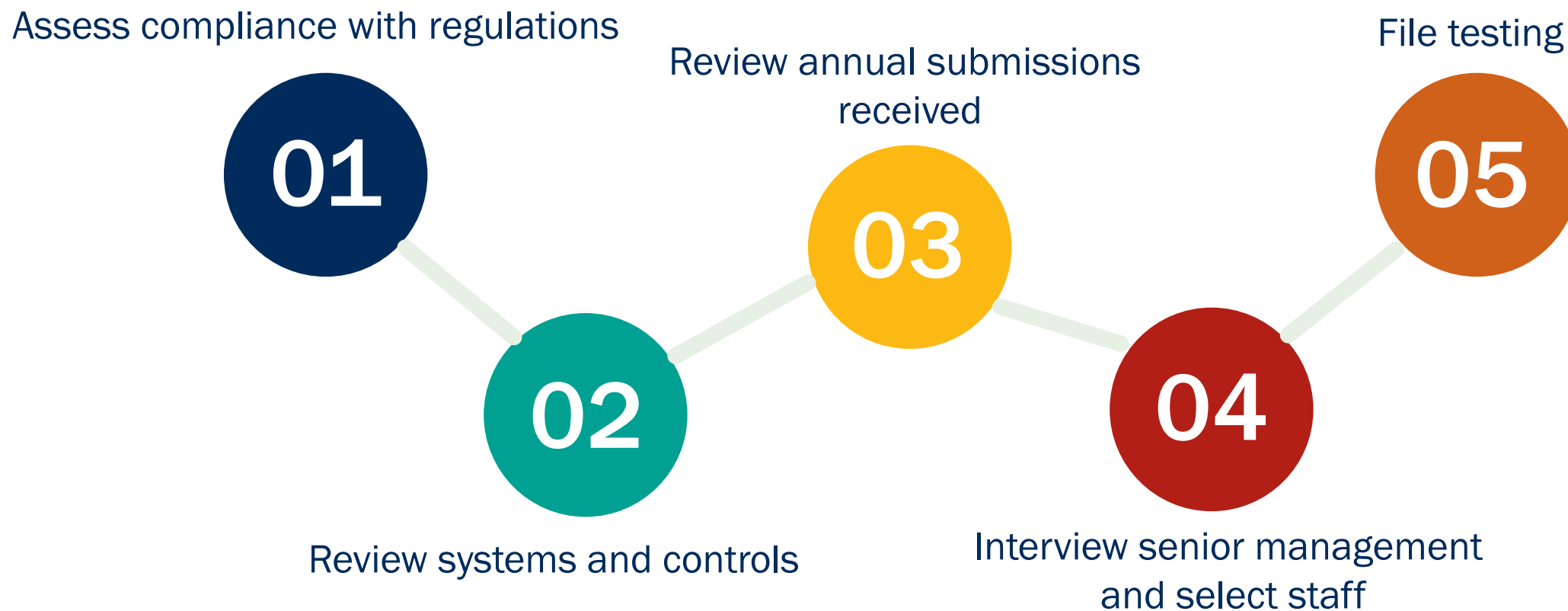


Customer Identification vs Verification Process

- In Bermuda, CDD regulations align with the Financial Action Task Force (FATF) guidelines, per FATF Recommendation 10
- The 2008 Proceeds of Crime AML/ATF Regulations (POCR) provide robust measures to combat Money Laundering/Terrorist Financing. Countries with similar legislation include the US, UK, Canada, Germany, Australia, India, France, Singapore, Brazil and South Africa
- Every Regulated Financial Institution (RFI) in Bermuda needs to have systems for identifying (collecting) and verifying (authenticating) information regarding customers during the CDD process
- RFIs can execute verification processes using varied methods: 'Documentary,' 'Electronic,' or 'Physical Verification'



AML/ATF Onsite Examination Process



Sector-specific Resources

Resource Guidance	Links
FATF Guidance:	Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (fatf-gafi.org) Guidance on Digital ID Red Flag Indicators Report to G20 on So-called Stablecoins
Bermuda Laws and Regulations	https://www.bma.bm/viewPDF/documents/2023-11-14-11-11-48-Digital-Asset-Business-Act-2018.pdf Digital Asset Issuance https://www.bermudalaws.bm/

Sector-specific Resources (Cont'd)

Resource Guidance	Links
Summary of key laws related to AML/ATF in Bermuda.	https://www.gov.bm/international-sanctions-measures https://www.gov.bm/sites/default/files/FSIU_Financial_Sanctions_Guidance_September_2021.pdf https://www.bma.bm/viewPDF/documents/2023-11-08-14-03-55-Proceeds-of-Crime-Anti-Money-Laundering-and-Anti-Terrorist-Financing-Regulations-2008.pdf https://www.bma.bm/viewPDF/documents/2023-11-08-14-05-27-Proceeds-of-Crime-Anti-Money-Laundering-and-Anti-Terrorist-Financing-Supervision-and-Enforcement-Act-2008.pdf https://www.bma.bm/viewPDF/documents/2023-11-08-14-06-43-Anti-Terrorism-Financial-and-Other-Measures-Businesses-in-Regulated-Sector-Order-2008.pdf https://www.bma.bm/viewPDF/documents/2023-11-08-14-07-22-Financial-Intelligence-Agency-Act-2007.pdf https://www.bma.bm/viewPDF/documents/2023-11-08-14-07-43-Anti-Terrorism-Financial-and-Other-Measures-Act-2004.pdf https://www.bma.bm/viewPDF/documents/2023-11-14-17-11-02-International-Sanctions-Regulations-2013.pdf

Sector-specific Resources (Cont'd)

Resource Guidance	Links
Bermuda Monetary Authority Guidance Notes	https://www.bma.bm/viewPDF/documents/2023-06-12-15-17-06-General-Guidance-Notes-for-AMLATF-Regulated-Entities-Revised.pdf
Specific guidelines provided by the regulatory authority	https://www.bma.bm/viewPDF/documents/2019-09-06-16-17-11-Annex-VIII-Sector-Specific-Guidance-Notes-for-Digital-Assets.pdf https://cdn.bma.bm/documents/2021-05-27-05-15-19-Digital-Asset-Business-FAQs-May-25.pdf
ML/TF NRA and AML/ATF General Guidance Notes Industry Outreach Session	https://www.youtube.com/watch?v=iuAN6poHamA
BMA Service Provider Training Course	https://www.bma.bm/viewPDF/documents/2022-09-06-11-42-02-FAQ--Service-Provider-Training.pdf

DAB Sector Outreach

Financial Intelligence Agency



FIA Agenda

01

SAR Filing Stats

02

DAB Trends and DAB Typology

03

Quality of SAR/STR Reporting

04

Reminders: SAR/STR Filings



DABs: Overview of SAR/STR Filings (2021-2024)

SAR/STR Filings (2021-2024)

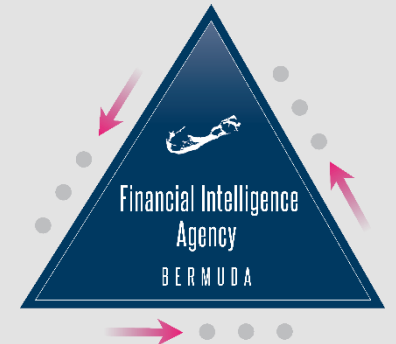
2021	2022	2023	2024 (Q1)	2024 (Q2)
14	352	206	116	54





DAB Trends

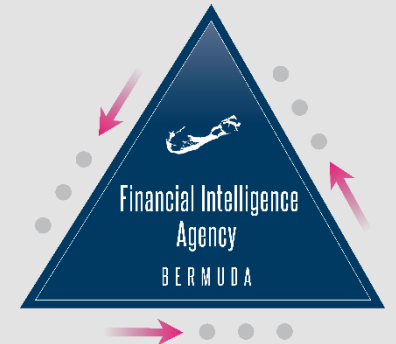
- There was exposure to addresses associated with mixing services
- The customer is avoiding requests for source of funds documentation and/or the source of funds is questionable
- The transactions had no apparent economic, business or lawful purpose
- There was exposure to addresses attributed to the darknet, sanctioned entities and/or gambling platforms
- Funds were sent off the platform within a short period of time





DAB Typology

The DAB sector detected direct and indirect receiving exposure to addresses attributed to NBCTF Seizures List, categorised as terrorist financing by a blockchain analytics company, in Person A's account. The NBCTF Seizures List is a list of cryptocurrency addresses identified by the National Bureau for Counter-Terror Financing of Israel as being associated with terrorist financing.



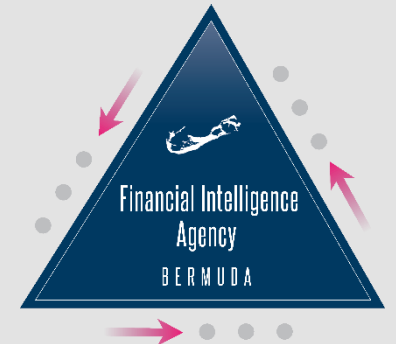
DABs: Quality of SAR/STR Filings

Overall Quality: Good

NB. Always provide supporting documents to support the SAR/STR narrative. Also, for consent requests, please provide all of the beneficiary wallet details.

Upcoming Action for the FIA:

To provide guidance on how to effectively submit STRs involving suspect transactional activity via manual inputting or XML upload and info needed for consent requests.





Reminders – SAR/STR Filings

1. Consent requests
2. Filing
3. Declined business
4. Refusal to provide Customer Due Diligence



DAB Sector Outreach - Takeaways

Focus on a risk-based approach to your AML ATF programme, specifically managing your highest risks including:

- Revising your Business Risk Assessment (BRA) annually and updating it when ML/TF risks change.
- Importance of Role of Compliance Officer and MLRO and providing appropriate AML/ATF training.
- Having an in-depth understanding of the Regulations (POCR) and Sanctions legislation and implementation of the same.
- Gap Analysis: Alignment of your AML ATF and Sanctions policies, procedures, and controls with the most recent POCR and related legislation.
- Outsourcing/Reliance: Importance of maintaining oversight and regularly monitoring those activities.

Remember that your Company **will be held accountable** for any failures associated with outsourcing, reliance or any other breaches in the POCR.



Questions and Answers

Email: AML@bma.bm (BMA) or info@fia.bm (FIA)