BMA
BERMUDA MONETARY AUTHORITY

Business Risk Assessment and Customer Risk Assessment

Presented by: AML/ATF Department – Elizabeth Awori

1 May 2025

Agenda

Introduction

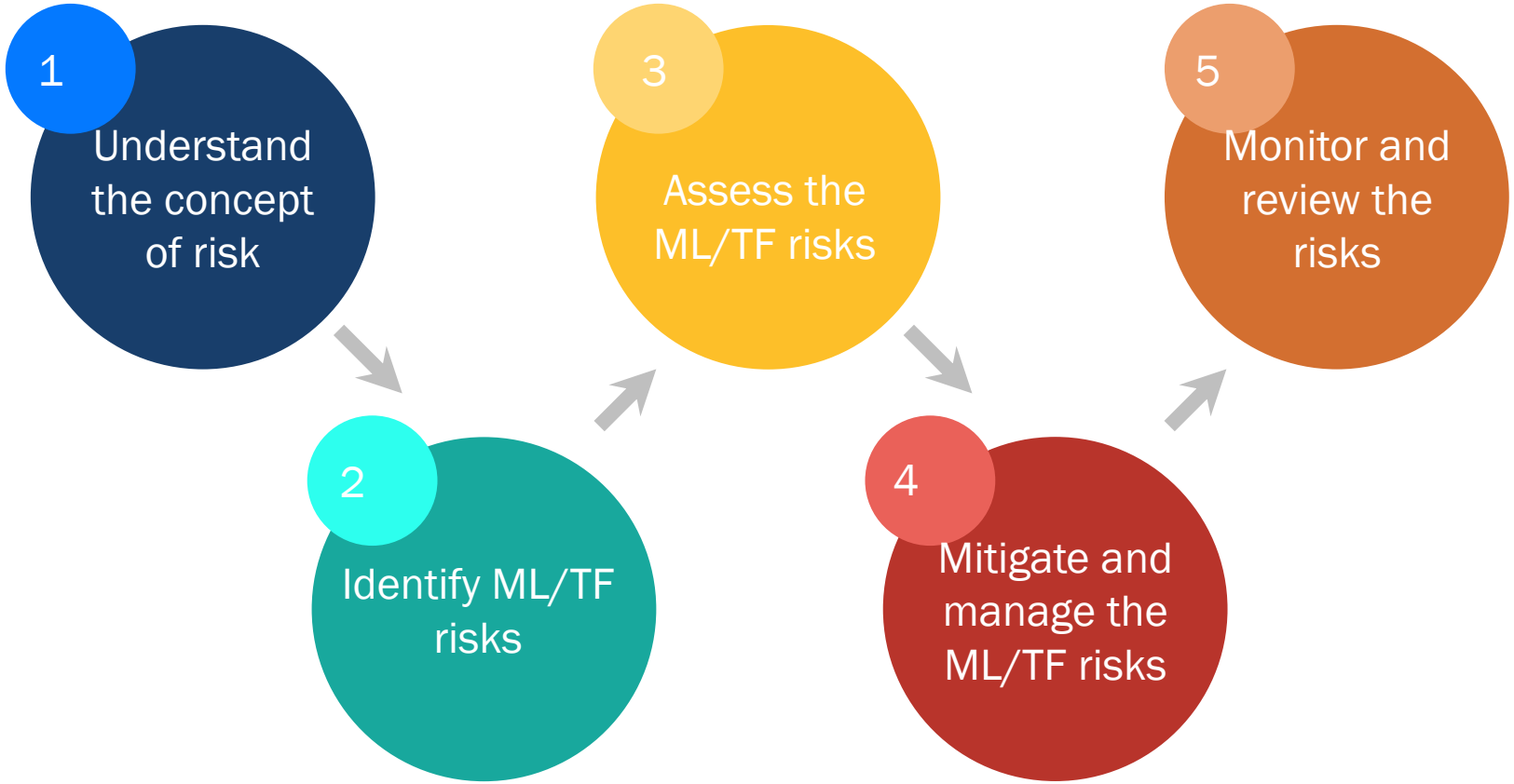
Objectives:

- Align the BRA and CRA to the Business Plan strategy
- Recognise that the BRA and CRA documents are essential in helping a Registered Financial Institution (RFI) implement a risk-based approach
- Ensure the alignment of risks between the BRA and CRA
- Emphasise that the RFI retains the ultimate responsibility for achieving the purpose of the documents (i.e., establishing its risk-based approach)
- Highlight BRA and CRA trends of non-compliance

Business Risk Assessment

PUBLIC

Stages of the Business Risk Assessment



3

Assess the ML/TF risks

Stages of the Business Risk Assessment

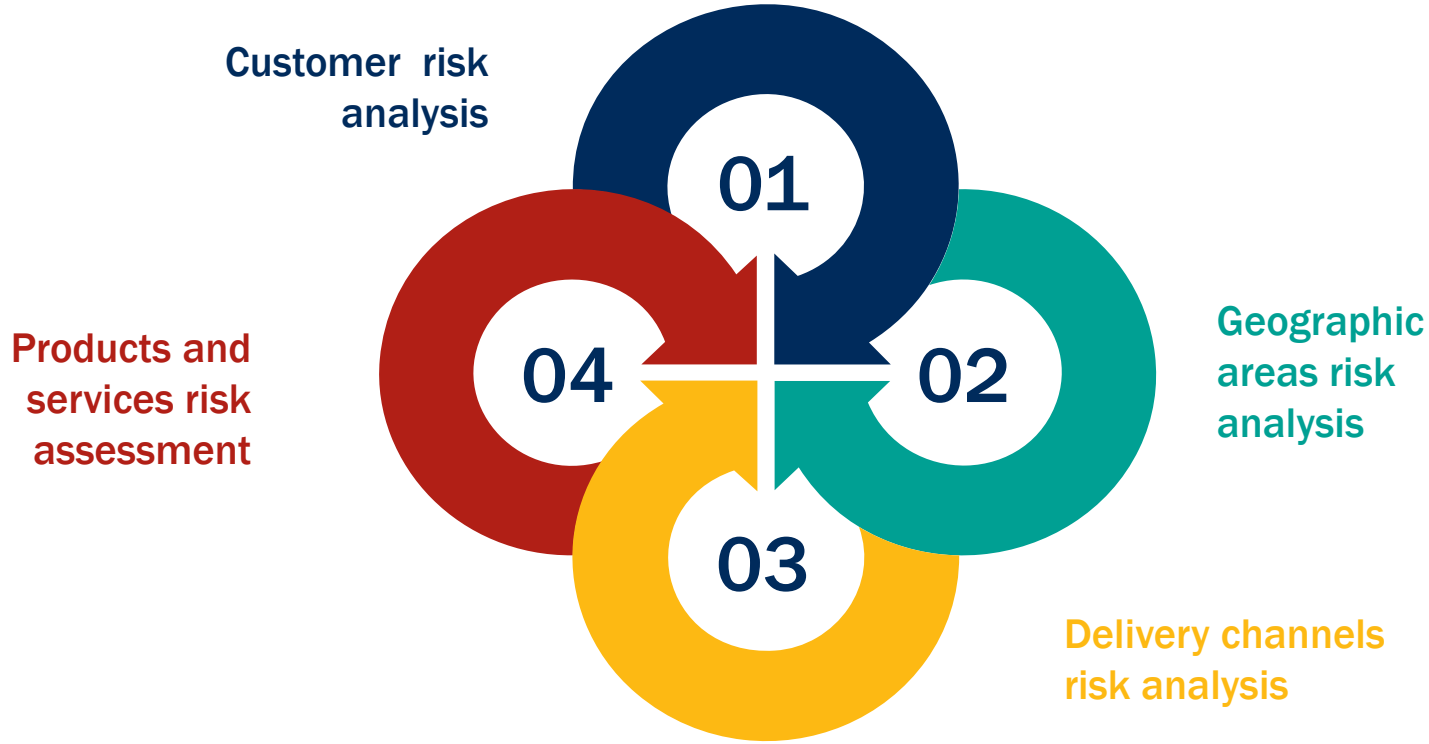
Customers	Geographic	Products or Services	Delivery Channels
Politically Exposed Person (PEP) status and adverse media	Country of incorporation and operations	Products/services that mask the origin or destination of funds	Face-to-face customer interactions
Source of funds and source of wealth	The origin and current location of the source of funds	Products/services that obscure the true identity of owner and/or beneficiary	Digital identification and verification
Complex and opaque ownership structures	Citizenship and residency of all named parties	Products/services used to conduct business within higher-risk industries or jurisdictions or on behalf of a third party	Via third-party intermediaries, agents or brokers
Occupation and/or industry	Any connections to high-risk jurisdictions	Products/services used to move funds to finance terrorist acts	Non-face-to-face customer acceptance or transacting

3

Assess the ML/TF risks

Stages of the Business Risk Assessment

The risk rating assignment is done through further assessments and analysis as follows:

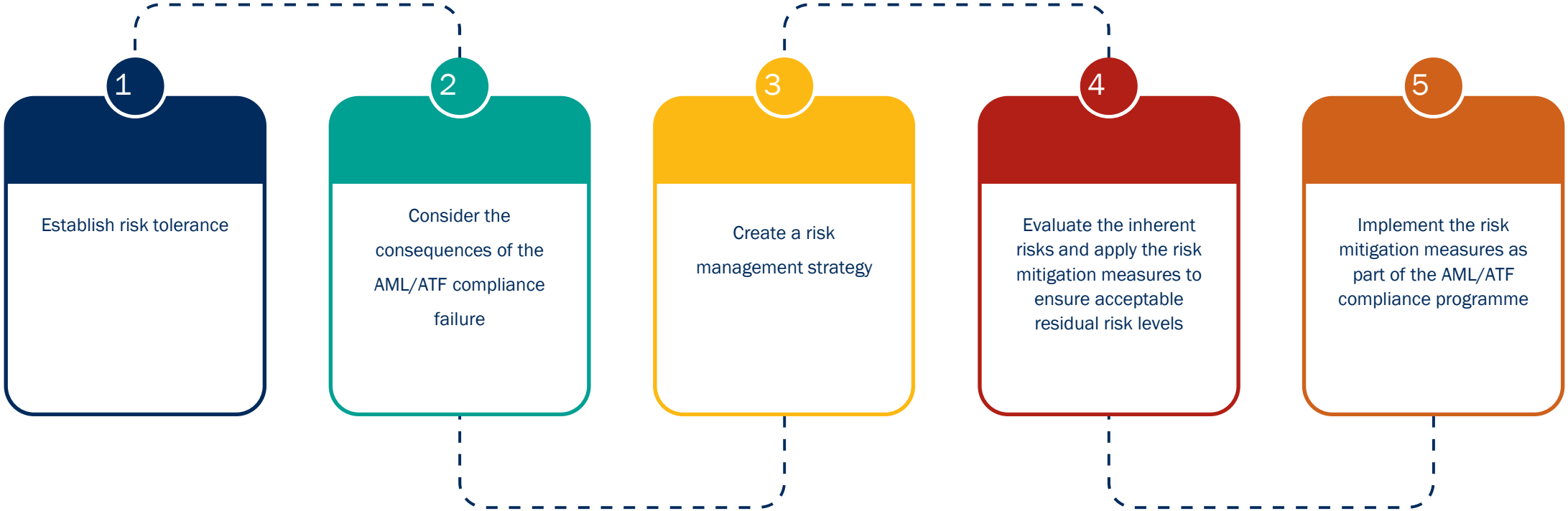


**An RFI must also perform a sanctions risk assessment, either separately or as part of its ML/TF BRA

4

Mitigate and manage the ML/TF risks

Stages of the Business Risk Assessment



5

Monitor and review the risks

Stages of the Business Risk Assessment

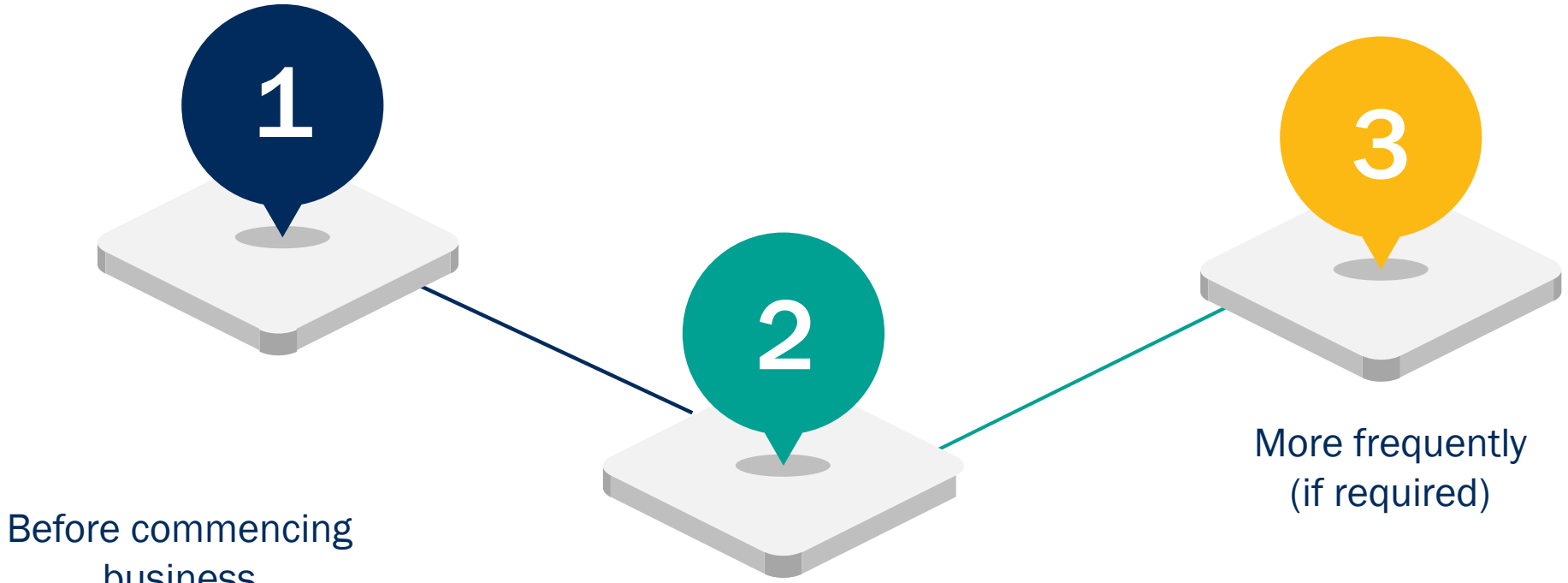
- Update the risk assessment to reflect the evolving risks. Each RFI should re-evaluate and update its risk-based approach regularly, and each time, the risk factors change

- Monitor the implementation of controls and enhance or improve them when needed

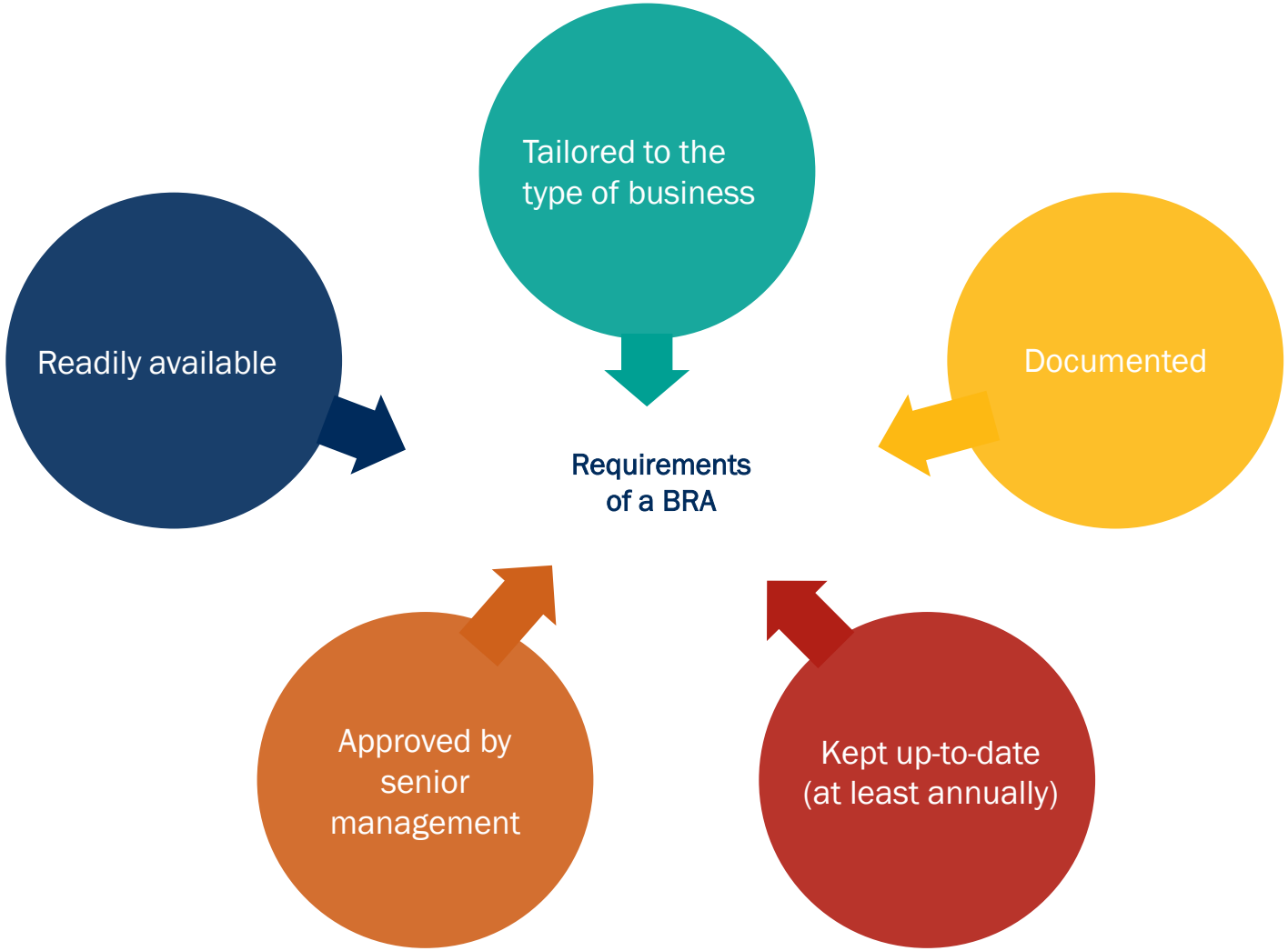
- Approval of policies, controls and procedures by senior management

Business Risk Assessment – Methods and Timing

The BRA methodology may be qualitative and/or quantitative and must be conducted:



Business Risk Assessment - Key Requirements



On-site/Off-site Examination – BRA Trends of Non-compliance

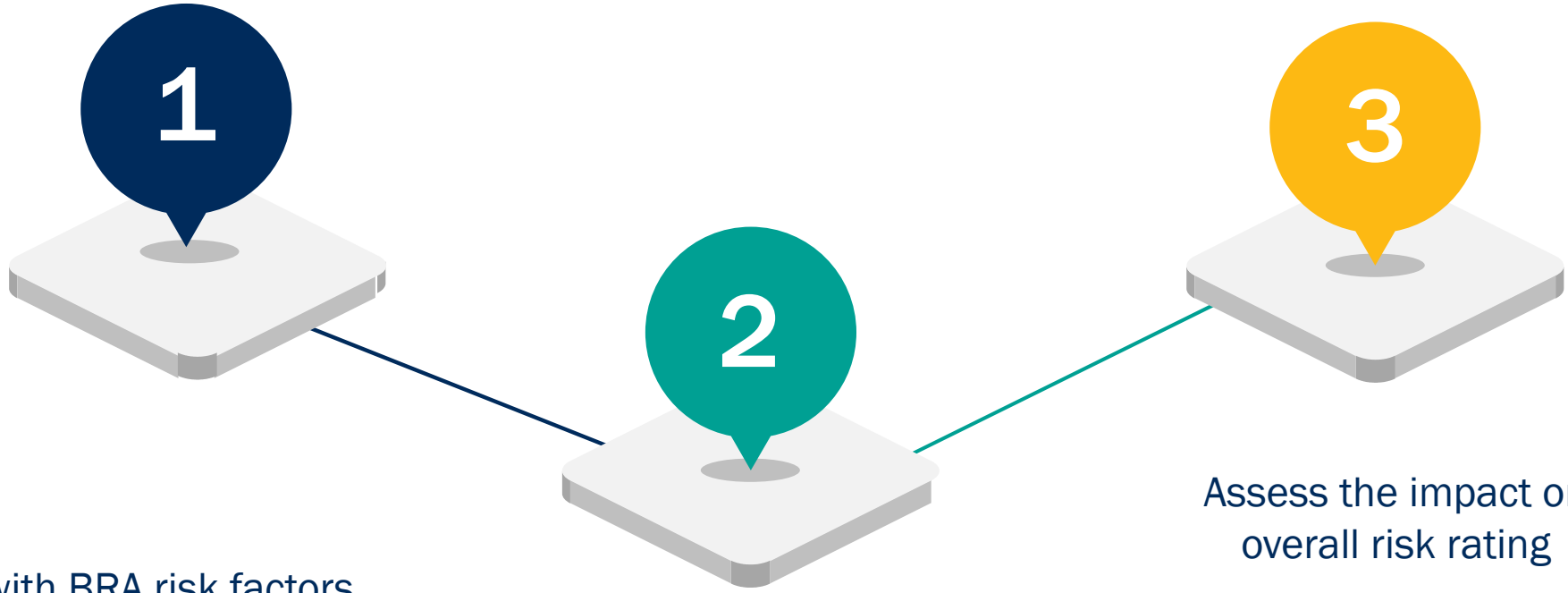
- Non-consideration of all the relevant business risks including Bermuda's National Risk Assessment results
- Risks noted not commensurate with the nature, scale and size of the business
- Inherent risks, controls and residual risks not clearly stated
- Risk factors noted do not align with the CRA and products and services risk assessment
- Inadequately defined controls which are not specific to the inherent risks identified
- Complicated BRAs that are either not fully understood by the RFI
- Oversimplified BRAs that do not represent all the risks of the RFIs
- Not updated on a regular basis or in line with the evolving risks
- Lack of accountability and ownership of the process and the BRA results
- Non-inclusion in the independent audit examination

Customer Risk Assessment

PUBLIC

Customer Risk Assessment - Key Requirements

The CRA methodology may be qualitative and/or quantitative and must:



Align with BRA risk factors

Consider threats and vulnerabilities to each customer

Assess the impact on overall risk rating

Customer Risk Assessment – Key Requirements

The CRA tool/form must:

- Align with the BRA
- Consider all risk factors
- Be tested and updated frequently
- Be sensitive to changes in the factors selected
- Allow flexibility
- Be dated and signed off (at the appropriate level)

A risk assessment for each customer must:

- Consistently use all inputs required by the tool/form
- Be dated and signed off (at the appropriate level)

On-site/Off-site Examination - CRA Trends of Non-compliance

- Does not consider all the relevant threats and vulnerabilities
- No guidance provided as to what each selected/noted response implies
- A CRA tool that is too complicated for the users to understand
- Incompleteness of the tool, whereby the user does not complete all the relevant fields in the CRA tool
- A CRA tool that is too simplified and does not capture all the risks of the customer
- A CRA tool that is not flexible enough to allow authorised updates to the factors noted
- A CRA tool that is vulnerable to manipulation by unauthorised users
- The functionality of the tool has not been tested
- A CRA tool that is neither dated nor signed (internal controls)
- Off-the-shelf CRA tools that are not applicable/relevant to the RFI
- Lack of ownership of the tool (where consultants or third parties are involved, the companies do not take accountability for the tools)
- Risk factors noted do not align with the BRA and products and services risk assessment

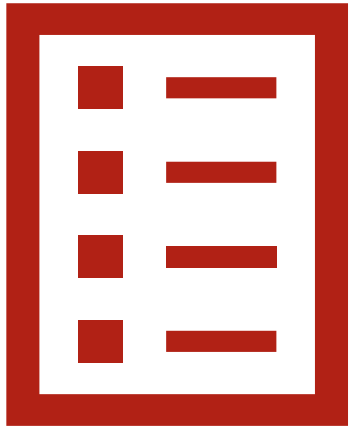
Case Studies

PUBLIC

Case Study – Business Risk Assessment in a Digital Asset Business (DAB)

1. ABC Ltd., a licensed DAB in Bermuda, offers a suite of digital asset services, including issuance, sale, redemption of digital assets, operation of an exchange and custodial wallet provision.
2. In early 2024, ABC Ltd. updated its BRA for Money Laundering/Terrorist Financing (ML/TF), adding mitigation that strictly prohibited transactions linked to sanctioned jurisdictions and those listed on the Financial Action Task Force's (FATF) grey and black lists.
3. When FATF expanded its 'Jurisdictions under Increased Monitoring' on 25 October 2024, ABC Ltd. should have responded by updating its ML/TF BRA and country list.
4. Despite introducing new potential risks based on the FATF update, ABC Ltd.'s Compliance Department failed to review its BRA in response to this 'trigger event'.
5. The Compliance Department relied on an outdated BRA thus potentially overlooking updated risks.

Case Study – Customer Risk Assessment in a Digital Asset Business



1. XYZ Ltd., a licensed DAB in Bermuda, specialises in digital asset services, including the issuance, sale and redemption of digital assets such as virtual coins and tokens, asset exchange and custodial wallet provision.
2. The company caters to an international customer base, offering various products and services. Their customers include nationals residing in different jurisdictions from their country of origin, with some holding dual nationalities or having been born and still having connections to FATF-blacklisted countries.
3. A significant issue arises with XYZ Ltd.'s CRA tool. It only captures the customer's nationality, neglecting factors such as the country of residence or dual nationality status.
4. The CRA tool also overlooks a factor that may influence the risk assessment: it doesn't account for the customer's country of birth and its associated connections, even if it is a FATF-blacklisted country.
5. The current CRA methodology reveals potential gaps in capturing comprehensive risk-related information, which may lead to a potentially skewed understanding of their risk profile.

Case Study – Customer Risk Assessment in a Trust and Corporate Service Provider Business

1. DEF is a Bermuda RFI holding a Trust and Corporate Service Provider (CSP) licence.
2. One of DEF's directors had a long-standing relationship with a corporate client and introduced them to DEF, which subsequently provided the client with various trust and CSP services. DEF decided to apply simplified due diligence due to this introduction and, therefore, did not collect all necessary Customer Due Diligence (CDD) or assign an appropriate risk rating to the corporate client.
3. It was noted that the corporate client was located in a high-risk foreign country and was involved in high-risk industries, including oil and mining.
4. At the time of the on-site it was identified that one of the shareholders had adverse media, while another shareholder was flagged as a foreign PEP.

Key Takeaways

PUBLIC

Key Takeaways

- Align the BRA and CRA with the Business Plan strategy
- The Business Plan, BRA and CRA are foundational documents
- The BRA and CRA risk factors must be in alignment
- RFIs retain ultimate responsibility for meeting the objectives of the BRA and CRA (ownership and understanding)
- The BRA and CRA must be evergreen documents

BMA
BERMUDA MONETARY AUTHORITY

Questions and Answers