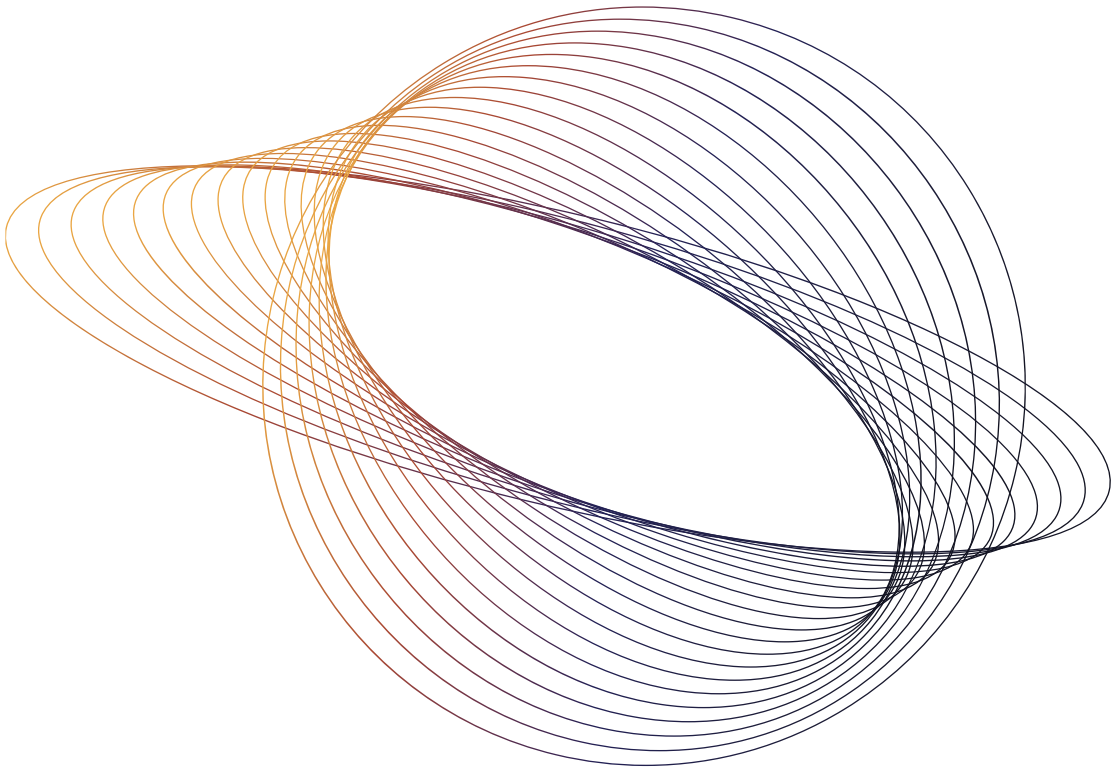
حكومة دبي
GOVERNMENT OF DUBAI

VARA
سُلطة تنظيم الأصول الافتراضية
VIRTUAL ASSETS REGULATORY AUTHORITY

AML/CFT Business Risk Assessment Guidance



varaconnect@vara.ae - صندوق بريد: 9292 دبي، الإمارات العربية المتحدة - سُلطة تنظيم الأصول الافتراضية
varaconnect@vara.ae - PO Box 9292, Dubai, UAE - Virtual Assets Regulatory Authority

AML/CFT Business Risk Assessment

Good Practice Guidance for Virtual Asset Service Providers

This guidance is published by VARA for the benefit of licensed virtual asset service providers and is intended to illustrate characteristics of strong AML/CFT Business Risk Assessment practice, drawing on VARA's supervisory observations from the 2026 BRA thematic review.

1. Introduction

A well-constructed AML/CFT Business Risk Assessment ("BRA") is the foundation of an effective financial crime compliance programme. It enables a VASP to identify the specific money laundering ("ML"), terrorism financing ("TF"), proliferation financing ("PF") and associated risks inherent to its business model, assess the effectiveness of its controls against those risks and make informed decisions about where to direct compliance resources. A BRA that is thorough, evidence-based and operationally connected to daily control decisions is a critical indicator of a mature AML/CFT programme.

Under Rule III.D of the VARA Compliance and Risk Management Rulebook ("Rulebook"), licensed VASPs must conduct and maintain an AML/CFT business risk assessment. The BRA must be reviewed at intervals of no longer than three months and must be updated whenever a significant change occurs in any of the areas listed in Rule III.D.2 (Rule III.D.3). VASPs must also be able to demonstrate to VARA that BRA outcomes directly inform the development and update of AML/CFT policies, procedures, systems and controls, and the prioritisation of resources in AML/CFT activities (Rule III.D.4). The BRA must reflect the VASP's specific business activities, customer base, product set, geographic footprint and the broader UAE threat environment as reflected in the UAE National Risk Assessment, relevant sectoral risk assessments and FATF guidance.

Purpose of this guidance

This document sets out good practice characteristics for AML/CFT Business Risk Assessments, drawing directly on VARA's supervisory observations from the 2026 BRA thematic review. It is intended to assist licensed VASPs in strengthening their BRA frameworks and to provide a clear picture of what robust, effective practice looks like in the UAE virtual assets sector.

The guidance is illustrative. VASPs should develop BRA frameworks that reflect their specific business model, risk profile and scale. The characteristics described in this document are drawn from actual practice observed across the licensed population.

Terms used in this guidance have the meanings given to them in the VARA Compliance and Risk Management Rulebook. Readers are referred to Schedule 1 of the Rulebook for defined terms.

The BRA thematic review

VARA conducts periodic sector wide BRA thematic reviews covering all licensed VASPs, using a dual methodology: a structured questionnaire covering BRA governance, scope, methodology, data inputs, inherent risk coverage, proliferation financing integration, control effectiveness assessment, operationalisation and review cycle; and a detailed supervisory analysis of BRA documents submitted by VASPs. The questionnaire covers eight thematic areas: governance and senior management accountability; scope and methodology; data sources and evidential grounding; inherent risk category coverage; proliferation financing treatment; control effectiveness assessment; operationalisation of BRA findings; and review cycle and version control. The document analysis examines how VASPs implement their stated methodology in practice, i.e. how they integrate quantitative evidence into risk scoring, how they treat PF as a distinct risk category and how they translate BRA findings into operational AML/CFT decisions.

As at early 2026, BRA capability across the licensed population is developing. A number of VASPs have invested in sophisticated, data driven frameworks that demonstrate genuine risk-based thinking calibrated to the UAE threat environment. This guidance draws on those examples to illustrate what strong practice looks like.

2. Governance and senior management accountability

An effective BRA must be anchored in the VASP's governance framework. The level of Board engagement with the BRA - including active challenge of methodology, residual risk conclusions and remediation priorities - is one of the strongest indicators of BRA maturity.

Board approval and ownership

Strong practice requires the BRA to be formally approved by the Board of Directors or an equivalent governing body, with the approval documented including the specific date on which it was given. Approval at senior management level alone does not provide the same quality of independent challenge or governance accountability.

The MLRO typically owns the BRA and is responsible for its preparation, maintenance and accuracy. However, MLRO ownership does not substitute for Board level approval: the Board's role is to provide independent challenge of the MLRO's conclusions, particularly regarding residual risk ratings, control effectiveness assumptions and the adequacy of the risk appetite framework. VASPs demonstrating strong governance practice maintain a clear record of when the BRA was approved, by whom, and what substantive discussion or challenge was undertaken at the point of approval.

Three lines of defence

Robust BRA governance applies the three lines of defence model consistently. The compliance and MLRO function prepares the BRA and owns its content. The risk function or Board provides independent challenge. Internal audit independently validates the BRA methodology and the control effectiveness assumptions on which residual risk ratings are based. Where internal audit capacity is limited, an independent external party may perform this function on a risk-based cycle.

VASPs that rely solely on Board presentation as the independent review mechanism without internal audit or equivalent coverage of BRA methodology and control ratings operate with a single challenge mechanism. Board challenge is essential, but it benefits from being complemented by independent technical validation of the underlying methodology and control assessments.

Good practice example: responding to supervisory feedback

Following a VARA supervisory inspection, the VASP immediately escalated the inspection findings to its Board, obtained Board approval for a remediation plan and contracted an independent third party auditor to review its AML/CFT framework including the BRA methodology. The audit engagement was notified to VARA. Progress against the remediation plan is tracked through a milestone log appended to the BRA, with quarterly milestone updates evidencing completion of key actions. This approach is consistent with strong three lines of defence practice and demonstrates how supervisory engagement can strengthen BRA governance.

Escalation and incident governance

The BRA governance framework should specify how material changes to the risk environment – such as adverse inspection findings, significant typology developments, or changes in the UAE sanctions environment – are escalated to the Board and how such events trigger a BRA update.

3. Methodology: scope, structure and scoring

The methodology underpinning the BRA determines whether risk conclusions are transparent, repeatable and independently verifiable. A sound methodology enables the VASP to explain how it arrived at any given risk rating, demonstrate that comparable risks are rated consistently and update ratings systematically when inputs change.

Scope of the BRA

A BRA should cover all legal entities within the VARA VASP's licensed group, all VARA licensed activities and product lines and all jurisdictions in which the VARA VASP operates or has clients. Where the VASP is part of an international group, the local UAE BRA should clearly document the relationship between the group wide risk assessment and the UAE entity's own risk profile and should specifically address UAE specific typologies, local regulatory expectations and the extent to which local controls are operationally effective independently of group infrastructure.

Where group wide systems and infrastructure are relied upon – for example, where KYC, transaction monitoring or sanctions screening are performed by a group entity – the BRA should assess the residual risk associated with that dependency and document how local MLRO oversight is exercised to verify that group controls are effective for the UAE entity's specific risk profile.

Documented methodology

The BRA methodology should be formally documented and should address: the risk categories assessed; the inherent risk scoring scale and how scores are assigned; how control effectiveness is rated; how inherent risk and control effectiveness interact to produce residual risk; and how individual category ratings are aggregated into an overall BRA risk position. A documented methodology enables the BRA to be consistently applied across review cycles and independently validated.

Quantitative scoring and aggregation

VASPs demonstrating strong methodology practice use numerical scoring scales with defined ranges – for example, a five point likelihood scale and a five point consequence scale producing a numerical inherent risk score for each category. Control effectiveness is rated on a defined scale. Residual risk is derived from the interaction of inherent risk score and control effectiveness rating, mapped through a documented heat map or conversion table.

Individual risk category scores should be aggregated into an overall BRA risk rating. An overall rating enables the VASP, its Board and its supervisor to understand the entity level risk position at a glance and to track how that position changes between review cycles. Where weighted aggregation is used, the weighting rationale should be documented and reflect the VASP's actual risk profile.

Good practice example: quantitative scoring and aggregation

Strong submissions used numerical scoring matrices – typically a five point likelihood and consequence scale – producing inherent risk scores across a large number of typologies, grouped into weighted risk categories. Weightings were documented with a rationale reflecting where the VASP's most material risk concentrations sit, with products, customers and geography typically carrying the highest weights. Category scores were aggregated through a documented heat map into an overall inherent and residual risk rating, with control effectiveness rated on a defined multi-tier scale. This transparency means any individual score can be traced from its underlying inputs through to the overall rating, allowing the methodology to be independently validated.

The strongest submissions also assessed ML and TF separately before aggregation. Where a management or compliance overlay and discretion was applied to adjust a quantitatively derived residual rating, the rationale was documented and explained – for example, concluding a Medium overall residual on the basis that residual concentrations sit in the most material financial crime risk areas rather than being evenly distributed. This demonstrates both methodological soundness and appropriate use of senior compliance judgement.

Qualitative ratings and narrative support

Where qualitative risk ratings are used rather than numerical scores, each rating should be supported by documented narrative explaining the risk factors that drove the rating, the controls assessed, and the rationale for the residual risk conclusion. A BRA that records ratings without supporting narrative limits transparency and cannot be effectively challenged by the Board or an independent reviewer. Even without numerical scoring, the logic behind an overall risk characterisation should be documented, for example, explaining why a combination of High customer risk and Medium product risk produces a Medium-High overall inherent position.

4. Data integration and evidential support

A BRA that is not informed by quantitative operational evidence is, at best, a judgement. The strongest BRAs treat operational data as direct inputs to risk scoring, such that risk ratings respond to changes in the underlying data.

Operational data as scoring inputs

The following data categories should be incorporated as inputs into inherent risk and control effectiveness assessment:

- Customer risk rating distribution: the proportion of customers in each risk tier and how this has changed since the previous BRA.
- Transaction monitoring alert data: total alert volumes, alert to investigation conversion, escalation rates and SAR/STR conversion ratios.
- STR/SAR trends and volumes, including the financial crime typologies identified.
- Sanctions screening outcomes: the number of alerts generated, confirmed matches (if any) and disposition outcomes.
- Product volumes and transaction data, including geographic distribution of transaction flows.
- Customer nationality and geographic concentration data, with specific analysis of exposure to high-risk jurisdictions.
- Any internal audit findings and regulatory or supervisory feedback affecting the assessed effectiveness of specific controls.
- Offboarding and EDD statistics evidencing risk-based application of CDD controls.

NRA and external typology integration

The UAE NRA, FATF high-risk jurisdiction lists, FATF typology reports, MENAFATF guidance and UAE FIU strategic analysis publications should be explicitly referenced in the BRA with their findings reflected in the inherent risk assessment. Where a new NRA is published, a new FATF update is issued or a significant typology development occurs, the BRA should document how that development has been reviewed and whether it has changed any risk rating.

Good practice example: NRA and external typology integration (as at early 2026)

One VASP's BRA explicitly incorporated the current UAE NRA, the most recent UAE FIU strategic analysis report, the latest FATF high risk jurisdiction list update and current UAE legislative amendments. A dedicated section addressed a significant regional geopolitical development, documenting the VASP's review of its controls in light of that development and confirming the assessed impact on the BRA. The version control log recorded each regulatory development reviewed, the date of review and the assessed impact on risk ratings demonstrating that the BRA is a genuinely current document.

5. Inherent risk assessment

Coverage of inherent risk categories should reflect the specific characteristics of the VASP's business model. Standard risk categories, such as customer types, products and services, delivery channels, geographic exposure and transaction volumes, are the minimum baseline. VASPs should also formally assess a set of VA specific risk categories not typically present in traditional financial services risk assessments.

VA specific risk categories

Strong BRAs in the virtual assets sector formally score each of the following categories:

- Unhosted wallets – the risk of transactions with unhosted wallets, including blockchain analytics coverage, UAE Travel Rule requirements and the VASP's policy on unhosted wallet interactions.
- Anonymity enhanced VAs and transactions (AETs) including privacy coins and mixing services. The BRA should address whether the VASP is exposed to transactions involving AETs and how associated risks are mitigated.
- DeFi and complex VA structures including decentralised exchange activity, smart contract interactions and products involving non-custodial or protocol-level intermediaries.
- Cross-border VA transfers including counterparty VASP exposure to high-risk jurisdictions and Travel Rule data integration into sanctions screening.
- Stablecoin specific risks reflecting current typology findings on the prevalence of stablecoins in on-chain illicit activity. The BRA should address stablecoin transaction volumes, counterparty exposure and associated PF and sanctions evasion risks.
- Emerging fraud typologies including AI enabled identity fraud, synthetic identity misuse, deepfake based account takeover and investment scam activity, which are increasingly prevalent in the virtual assets sector.

Geographic risk

Geographic risk assessment in the virtual assets sector requires more granularity than is typical in traditional financial services. VASPs should assess geographic risk at the level of individual jurisdictions, identifying the specific proportion of their customer base from each high-risk jurisdiction with reference to actual KYC nationality data.

Good practice example: geographic risk assessment

One VASP's geographic risk assessment identifies that a significant share of its UAE customers are from high-risk jurisdictions. The assessment provides a jurisdiction-by-jurisdiction breakdown with specific percentage figures for each high-risk jurisdiction, informed by customer nationality data from the VASP's KYC records. The overall geographic category carries a residual risk rating of High, which the VASP explicitly acknowledges and presents transparently to the Board, illustrating a BRA that presents a data informed picture of geographic risk.

6. Proliferation financing

Proliferation financing is a distinct financial crime risk category. FATF Recommendation 7 requires VASPs to implement targeted financial sanctions ("TFS") relating to PF without delay. The UAE's geographic context and the global reach of the virtual assets sector make PF a material risk for UAE licensed VASPs. Strong practice treats PF as a distinct risk category in the BRA with its own inherent risk score, control effectiveness assessment and residual risk rating, explicitly linked to the VASP's TFS operational framework.

PF as a distinct risk category

The BRA should assess PF risk separately from ML and TF with its own inherent risk scoring across the relevant risk dimensions. The primary PF risk vectors in the virtual assets sector are customer types (particularly corporate structures and customers with geographic links to proliferation sensitive jurisdictions) and geographic footprint (particularly exposure to DPRK and Iran). The BRA should also address PF specific evasion techniques: the use of nested accounts and intermediary VASPs; layered blockchain transactions; front companies and shell entity structures; and cross-chain bridge mechanisms used to obscure the origin and destination of funds.

PF-TFS operational linkage

The most important dimension of PF assessment is whether the BRA PF conclusions are demonstrably connected to the VASP's TFS operational framework, for example:

- How the PF risk rating informs the scope, frequency and calibration of TFS screening.
- Whether PF risk findings are reflected in TFS policies and procedures.
- Registration with the UAE Executive Office for Control and Non-Proliferation (EOCN) for receipt of PF related designation notifications.
- Procedures for implementing "without delay" asset freezing upon identification of a confirmed or potential TFS match, consistent with Cabinet Decision No. 74 of 2020.
- Reporting obligations through goAML for Confirmed Name Match Reports (CNMRs) and Partial Name Match Reports (PNMRs) following TFS matches.

Good practice example: PF assessment and TFS linkage

Strong submissions assessed PF as a distinct risk category with a high inherent risk rating, reduced to Medium residual through a documented control framework. The BRA documented the full operational chain between the PF risk assessment and TFS controls: EOCN Notification Alert System registration; real-time sanctions screening against the UN Consolidated List, UAE Local Terrorist List and DPRK and Iran-specific UNSC lists; without-delay asset freezing procedures; and reporting through goAML. The BRA explicitly stated how the PF inherent risk rating had driven the configuration of these controls.

PF specific controls documented across strong submissions: corporate structure risk mapping to identify front company and layered entity indicators; PF specific sanctions screening covering DPRK and Iran related UN designations; blockchain analytics for multi-hop transaction tracing designed to identify PF linked layering patterns and monitoring for AET activity associated with PF evasion. The TFS linkage, specifying how the PF risk rating informs screening calibration, was explicitly documented.

7. Control effectiveness assessment and residual risk

The quality of a BRA's residual risk conclusions depends entirely on the quality of its control effectiveness assessment. A residual risk rating derived from self-assessed control ratings without independent validation carries significant uncertainty. Good practice requires control effectiveness to be assessed with reference to objective evidence rather than judgement alone.

Evidence-based control effectiveness

Control effectiveness should be assessed with reference to:

- Internal audit findings addressing the design and operating effectiveness of specific AML/CFT controls.
- Results of independent compliance testing, including TM system testing, sanctions screening gap analysis and CDD/EDD quality reviews.
- Regulatory or supervisory findings where these have assessed the effectiveness of specific controls.
- Operational performance data such as TM alert closure rates, SAR/STR conversion rates, sanctions screening hit rates providing evidence of whether controls are operating as intended.

Where control effectiveness is self-assessed by the compliance or MLRO function without independent validation, the BRA should acknowledge this limitation. Self-assessed control ratings should be treated with appropriate caution in determining residual risk and the Board should be made aware of this limitation when approving the BRA.

Residual risk calibration

Residual risk conclusions should reflect the actual risk environment. The UAE NRA assesses the virtual assets sector as high risk for ML, TF and PF. VASPs should consider whether their residual risk ratings are consistent with that sectoral assessment. Strong practice recognises that structural inherent risk exposure cannot be fully eliminated through controls alone. Even where controls are mature and operating effectively, some residual risk will remain and the BRA should reflect this. Where judgement is applied to adjust a quantitatively calculated residual risk rating, the rationale should be documented and presented to the Board for approval.

8. Operationalisation: translating BRA findings into practice

A BRA that does not drive operational decisions is not a risk management tool. The value of a BRA is realised when its findings directly inform how the VASP manages its AML/CFT programme: which controls are enhanced, how TM alert thresholds are calibrated, where compliance resources are directed and which areas receive heightened oversight.

BRA findings as operational inputs

Strong BRAs document specific examples of how BRA findings have driven operational decisions in the preceding review cycle. These might include:

- A change to TM alert thresholds following a BRA finding that a specific product's inherent risk had increased.
- An enhancement to sanctions screening configuration, for example, an increase in the number of transaction hops assessed in blockchain analytics following a BRA conclusion that PF inherent risk had increased.
- A decision to apply EDD to customers from a specific jurisdiction, following a BRA finding that geographic inherent risk for that jurisdiction had increased due to a new FATF listing or geopolitical developments.
- A reallocation of compliance resources following a BRA finding that TM alert volumes in a specific business line were disproportionate to available investigation resources.
- A revision to CDD or EDD policy following a BRA finding that a specific customer type presented higher inherent risk than previously assessed.

The BRA should include a section documenting specific operational decisions in the most recent review cycle that were directly informed by BRA findings. This section provides the evidentiary link between the risk assessment and the compliance programme.

Trigger based BRA updates

The BRA should be updated when specific trigger events occur:

- New products, services or technologies, including new virtual asset listings.
- Material changes in the customer base or risk distribution.
- Regulatory or NRA updates, including new FATF jurisdiction listings or VARA supervisory communications.
- Adverse supervisory, audit or law enforcement findings.
- Sanctions designation of a counterparty VASP or a virtual asset listed on the platform.
- Material changes to the AML/CFT programme or key personnel, including MLRO changes.

9. Review cycle and version control

A BRA reviewed on a defined cycle and maintained with rigorous version control is demonstrably a live document. Version control provides the evidentiary basis for demonstrating that the BRA is updated in response to a changing risk environment.

Review frequency

VASPs must review and update the BRA at intervals of no longer than three months (Rule III.D.3 of the Rulebook) . Each quarterly review should be substantive incorporating updated operational data, an assessment of any external developments and a review of whether any risk ratings have changed since the previous version. Unchanged ratings across all categories should be accompanied by documented rationale explaining why stability reflects the actual risk environment.

Version control and change logs

Best practice maintains a granular version control log documenting: the date of each version; the author and approval body; the specific changes made from the previous version; the regulatory or operational development that prompted each change and the assessed impact on risk ratings. A change log that records not only what changed but why with reference to a specific external development or internal finding demonstrates that the BRA is responsive to the risk environment.

Good practice example: version control and change narrative

Strong submissions maintained the BRA across multiple versions, with a change log recording the specific regulatory development or operational change that prompted each revision, the sections of the BRA affected and the assessed impact on risk ratings. New regulatory developments are recorded in the change log with a documented impact assessment, even where the assessment concludes that no rating change is required. This provides a clear audit trail demonstrating that external developments are being monitored and assessed on a continuous basis.

Strong submissions also tracked the evolution of the risk profile across versions, noting where risk ratings have changed with an explanation of the drivers. Where a residual risk increase from the previous version was attributed to methodological enhancement rather than a deterioration in the risk environment, e.g. following supervisory engagement that prompted more granular scoring, this was clearly explained. This transparent narrative enables the Board and supervisor to assess whether rating changes reflect genuine risk developments or methodology changes.

10. Conclusion

BRA frameworks are becoming embedded across the VARA ecosystem. The strongest submissions demonstrated that a well constructed BRA is a live risk management tool that is grounded in operational data, responsive to the external threat environment, subject to independent challenge and directly connected to how the VASP manages its AML/CFT programme day to day. VARA encourages all licensed VASPs to use this guidance to assess the maturity of their BRA frameworks and to identify areas for further development. VARA will continue to assess BRA quality as part of its ongoing supervisory engagement.