RISK ASSESSMENT AND SCORING POLICY

Company	**GoldTakas FZCO**
Jurisdiction	United Arab Emirates – Dubai / DMCC
Version / Date	2.0 / 28.08.2026
Effective Date	01/09/2026
Document Owner	MLRO / Compliance Function
Approval Authority	Senior Management

This policy shall be read in conjunction with GoldTakas FZCO's primary AML/CFT Policy. Rather than duplicating provisions related to training, record-keeping, and the overall compliance program, this document defines the methodology for risk identification, classification, scoring, acceptance/rejection decisions, and the determination of monitoring intensity.

1. PURPOSE

The purpose of this policy is to ensure that GoldTakas FZCO assesses AML/CFT risks arising from its clients, transactions, geographic exposures, products and sectors, and third-party relationships in a systematic, consistent, measurable, and auditable manner.

The policy supports the implementation of a risk-based approach, the calibration of control intensity in line with risk levels, and the appropriate escalation of high-risk relationships.

2. SCOPE

This Policy applies to all prospective and existing clients, including:

- Individuals;
- Corporate entities;
- Financial institutions;
- Refineries;
- Precious metals dealers and traders;
- Intermediaries;
- Suppliers; and
- Other relevant third parties.

The Policy applies throughout the client lifecycle, including onboarding, ongoing monitoring, periodic review and event-driven reassessment.

3. REGULATORY AND REFERENCE FRAMEWORK

This Policy has been developed with reference to applicable UAE legal and regulatory requirements and relevant international standards, including:

- UAE Federal AML/CFT legislation and implementing regulations;
- UAE Targeted Financial Sanctions requirements;
- FATF Recommendations and Guidance;
- DMCC AML/CFT and compliance requirements applicable to Dealers in Precious Metals and Stones (DPMS);
- OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas;
- LBMA Responsible Gold Guidance;
- applicable United Nations Security Council sanctions regimes; and
- relevant international good practices for financial crime risk management.

Where applicable legal or regulatory requirements are more stringent than this Policy, such requirements shall prevail.

4. DEFINITIONS

For the purposes of this Policy:
AML/CFT: Anti-Money Laundering and Counter-Terrorist Financing.
CAHRA: Conflict-Affected and High-Risk Area.
CDD: Customer Due Diligence.

Client: Any individual or legal person establishing or seeking to establish a business relationship with GoldTakas FZCO.
EDD: Enhanced Due Diligence.
Final Risk Classification: The ultimate risk classification assigned to a Client after application of the methodology established under this Policy, including any applicable High Risk Override.
High Risk Override: A circumstance requiring a Client to be classified as High Risk irrespective of the quantitative risk score.
Inherent Risk: The level of risk before consideration of eligible mitigating controls.
ML/TF/PF: Money Laundering, Terrorist Financing and Proliferation Financing.
PEP: Politically Exposed Person.
Residual Risk: The level of risk remaining after eligible mitigating controls have been considered.
SoF: Source of Funds.
SoW: Source of Wealth.
UBO: Ultimate Beneficial Owner.
Zero Tolerance: A circumstance involving a legal prohibition or risk outside the Company's approved risk appetite for which the relationship or activity may not be accepted or continued, subject to applicable legal and regulatory requirements.

5. RISK-BASED APPROACH

GoldTakas FZCO applies a Risk-Based Approach ("RBA") to identify, assess and manage AML/CFT risks.

Clients and business relationships shall be assessed based on relevant risk factors, including:

- Client characteristics and business activities;
- Geographic exposure;
- Products, services and transaction characteristics;
- Source of Funds and Source of Wealth;
- Ownership and control structure;
- Third-party involvement; and
- Supply chain and provenance risks, where applicable.

The level of due diligence, approval, monitoring and review shall be proportionate to the assessed risk. Higher-risk relationships shall be subject to enhanced controls, while lower-risk relationships may be subject to standard controls where permitted by applicable requirements.

The quantitative scoring methodology and applicable overrides are set out in Sections 8, 9 and 10 of this Policy.

6. GOVERNANCE AND RESPONSIBILITIES

The risk assessment and scoring framework shall be subject to appropriate governance, oversight and segregation of duties.

Senior Management shall retain overall responsibility for approving the risk-rating methodology and material amendments, while the MLRO / Compliance Function shall oversee its implementation, maintenance and consistent application.

Detailed roles and responsibilities relating to the governance, application, validation and independent review of the risk-rating framework are set out in Section 17 of this Policy.

Commercial considerations shall not override applicable legal or regulatory requirements, Zero Tolerance criteria or Compliance risk determinations.

7. DATA SOURCES AND ASSESSMENT INPUTS

GoldTakas FZCO shall base its risk assessments on information that is relevant, reliable, current and, where appropriate, independently verifiable.

Risk assessment inputs shall include, as applicable:

- Client identification and KYC/CDD information;
- Legal form, ownership and control structure, including UBO information;
- Sanctions, PEP and adverse media screening results;
- Source of Funds and Source of Wealth information;
- Expected and actual transaction profile and payment methods;
- Geographic and jurisdictional exposure;
- Business and sector characteristics;
- Third-party and intermediary involvement; and
- Supply chain, provenance and traceability information relevant to precious metals activities.

Where information material to the risk assessment is incomplete, inconsistent or cannot be satisfactorily verified, the matter shall be escalated in accordance with the applicable CDD/EDD, High Risk Override and Client Acceptance requirements.

7.1 Geographic Risk Inputs

Geographic risk shall be assessed using relevant and current indicators, including, where applicable:

- FATF country classifications;
- Applicable sanctions restrictions;
- Corruption and governance indicators;
- Offshore or secrecy-related jurisdictional characteristics; and
- CAHRA exposure relevant to precious metals activities.

These indicators shall be reflected through the quantitative scoring methodology or, where the applicable criteria are met, through the Zero Tolerance or High Risk Override framework.

Detailed sanctions screening, CDD and responsible sourcing controls shall be governed by the relevant Company policies and procedures.

8. RISK ASSESSMENT METHODOLOGY

GoldTakas FZCO shall apply a documented and consistent methodology to assess and classify Client risk.
The methodology consists of the following components:

1. Zero Tolerance / Prohibited Risk assessment;

2. High Risk Override assessment;
3. Quantitative Inherent Risk Assessment;
4. Application of eligible mitigating controls;
5. Determination of Residual Risk; and
6. Final Risk Classification.

Zero Tolerance and High Risk Override criteria operate independently from quantitative scoring and shall prevail where applicable.

8.1 Zero Tolerance / Prohibited Risk

Zero Tolerance applies where a Client, business relationship or transaction is prohibited by applicable law or regulation or falls outside the Company's approved risk appetite.

Zero Tolerance circumstances include, where confirmed:

- Applicable sanctions prohibitions or asset-freezing requirements;
- Terrorist financing or prohibited terrorist association;
- Intentional concealment of beneficial ownership or control;
- Fraudulent, forged or materially falsified information;
- Unlicensed activity where the relevant activity legally requires authorisation; and
- Other relationships or activities prohibited by applicable law or expressly designated by the Company as Zero Tolerance.

A screening alert, adverse media result or other unverified indicator shall not, by itself, constitute a confirmed Zero Tolerance determination.

Where Zero Tolerance applies:

- the relationship or activity shall not be established or continued, except where action is required to comply with applicable legal, regulatory, freezing, reporting or orderly exit requirements;
- quantitative scoring or mitigating controls shall not override the determination; and
- the matter shall be escalated in accordance with the applicable Company policies and procedures.

8.2 High Risk Override

A High Risk Override requires the Client or relationship to be classified as High Risk irrespective of the quantitative score, but does not, by itself, constitute a Zero Tolerance determination. The establishment or continuation of the relationship shall remain subject to all applicable legal and regulatory requirements and to the mandatory CDD, EDD and Client Acceptance requirements established under the Company's AML/CFT framework.

High Risk Override circumstances include:

- PEP exposure requiring High Risk treatment;
- inability to satisfactorily establish beneficial ownership or control after reasonable measures;
- materially unexplained or unverifiable Source of Funds;
- material CAHRA exposure requiring enhanced treatment; and
- credible and material criminal, regulatory or adverse information relevant to the relationship.

Where a High Risk Override applies:

- the Final Risk Classification shall not be lower than High Risk;
- EDD shall be mandatory;
- Senior Management approval shall be obtained where required;
- enhanced ongoing monitoring shall apply; and
- mitigating controls shall not reduce the Final Risk Classification below High Risk while the override remains applicable.

Where the underlying circumstances instead constitute a legal prohibition or Zero Tolerance criterion, the Zero Tolerance treatment shall prevail.

8.3 Quantitative Inherent Risk Assessment

Where neither a legal prohibition nor Zero Tolerance prevents the relationship from proceeding, the Client shall be assessed using the applicable Individual or Corporate scorecard under Sections 9 and 10.

The quantitative methodology operates on a **0–100 scale** and measures Inherent Risk before the effect of mitigating controls.

Unless otherwise specified, each quantitative risk factor shall be rated as follows:

Rating	Risk Level
0	Not Applicable / No Identified Risk
1	Low
2	Moderate
3	Elevated
4	High

A rating of 4 represents significant inherent risk but does not, by itself, constitute a High Risk Override or Zero Tolerance criterion.

Factor ratings shall be assigned on the basis of the criteria set out in the applicable Individual or Corporate scorecard and the information available through the Company's CDD, screening, transaction monitoring and other relevant control processes. Where the distinction between two ratings requires professional judgement, the selected rating and the material basis for that judgement shall be documented. The MLRO / Compliance Function may maintain supporting scoring guidance to promote consistent application of the methodology, provided that such guidance does not alter the approved rating scale, category weights, calculation methodology or classification thresholds established under this Policy.

8.4. Scoring Methodology

The quantitative risk assessment shall be performed using the approved factor ratings, Internal Factor Weights and Category Weights set out in the applicable Individual or Corporate scorecard.

Each applicable risk factor shall be assigned a rating in accordance with Section 8.3 of this Policy. The rating assigned to each factor shall then be multiplied by its applicable Internal Factor Weight to determine the Weighted Factor Rating.

Weighted Factor Rating = Factor Rating × Internal Factor Weight

The Weighted Factor Ratings within each risk category shall be aggregated to determine the Weighted Category Rating.

The Weighted Category Rating shall then be converted into the applicable Category Score by reference to the maximum factor rating of four (4) and the Category Weight assigned to that risk category:

Category Score = (Weighted Category Rating / 4) × Category Weight
The Category Scores shall be aggregated to determine the Client's Inherent Risk Score on a scale of 0–100:

Inherent Risk Score = Sum of all Category Scores
Where a factor is assessed as Not Applicable, it shall receive a rating of zero (0). The Internal Factor Weight assigned to that factor shall not be redistributed or re-normalised among the remaining factors within the relevant risk category.

The approved Category Weights are:

Individual Clients
- Customer / Relationship Risk: 30%
- Product / Transaction / Delivery Risk: 30%
- Geographic Risk: 25%
- Business / Sector Risk: 15%

Corporate Clients
- Customer / Ownership & Control Risk: 25%
- Product / Transaction / Delivery Risk: 25%
- Geographic Risk: 20%
- Business / Sector Risk: 15%
- Supply Chain / Provenance / Third-Party Risk: 15%

The resulting Inherent Risk Score shall be used as the quantitative starting point for the application of mitigating controls and the determination of the Residual Risk Score in accordance with Section 8.6 of this Policy.

The quantitative score shall not override or reduce the effect of any applicable Zero Tolerance criterion or High Risk Override. Where such criteria apply, the relevant mandatory outcome shall prevail irrespective of the calculated Inherent Risk Score.

8.5 Prevention of Double Counting
The same underlying risk circumstance shall not be inappropriately counted more than once.

In particular:

- a circumstance determining Zero Tolerance shall not also be quantitatively scored merely to increase the result;
- a High Risk Override shall not be duplicated through quantitative scoring where the same underlying risk is already determinative; and
- overlapping factors shall only be scored separately where they represent genuinely distinct risk exposures.

Where material overlap exists, the MLRO / Compliance Function shall determine the appropriate treatment.

8.6 Mitigating Controls and Residual Risk

Eligible mitigating controls may be applied only after the Inherent Risk Score has been calculated in accordance with this Policy.

A mitigating control may be recognised only where it is relevant to the specific risk being mitigated, demonstrably effective, supported by sufficient evidence and capable of ongoing verification.

For quantitative purposes, an eligible mitigating control may reduce the rating of the relevant risk factor by a maximum of **one (1) rating level**. A factor rating shall not be reduced below zero.

The cumulative effect of all mitigating controls shall not reduce the Inherent Risk Score by more than **fifteen (15) points**.

The Residual Risk Score shall be calculated as follows:
Residual Risk Score = Inherent Risk Score – Approved Mitigation Adjustment

The Approved Mitigation Adjustment shall be the lower of:
a. the aggregate score reduction resulting from the approved one-level factor rating reductions; or
b. fifteen (15) points.
Mitigating controls shall not:

- override a Zero Tolerance determination;
- reduce a Client subject to a High Risk Override below High Risk;
- compensate for incomplete or inadequate mandatory CDD or EDD;
- compensate for unresolved material UBO, SoF/SoW, sanctions, PF, provenance or responsible sourcing concerns;
- be applied where the effectiveness of the control cannot be reasonably demonstrated; or
- be applied solely because of the commercial importance of the relationship.

Each mitigating control and any resulting quantitative adjustment shall be documented together with the supporting rationale and evidence and shall be subject to review by the MLRO / Compliance Function.

Where a mitigating control ceases to be effective or can no longer be adequately evidenced, the relevant risk factor shall be reassessed and the Residual Risk Score recalculated without undue delay.

8.7 Final Risk Classification

The following hierarchy shall apply:

Legal Prohibition / Zero Tolerance → High Risk Override → Quantitative Inherent Risk Assessment → Eligible Mitigation → Residual Risk Score → Final Risk Classification

Where neither Zero Tolerance nor a High Risk Override applies, the Final Risk Classification shall be determined based on the Residual Risk Score as follows:

Residual Risk Score	Final Risk Classification
0.00 – 34.99	Low Risk
35.00 – 64.99	Medium Risk
65.00 – 100.00	High Risk

Where a High Risk Override applies, the Final Risk Classification shall be High Risk irrespective of the quantitative score, and no mitigating control shall reduce the classification below High Risk.

Where Zero Tolerance applies, the relationship or activity shall not be accepted or continued, subject to applicable legal, regulatory, freezing, reporting or orderly exit requirements. No quantitative score or mitigating control shall alter a Zero Tolerance determination.

The applicable classification thresholds form part of the approved risk-rating methodology and shall apply consistently to both Individual and Corporate Clients.

Any change to the classification thresholds shall constitute a material methodology change and shall be subject to documented testing and Senior Management approval in accordance with Section 15.

8.8 Control Response

The Final Risk Classification shall determine the minimum level of due diligence, approval, monitoring and review applicable to the relationship.

As a general principle:

- **Low Risk:** Standard CDD and proportionate ongoing monitoring;
- **Medium Risk:** CDD with additional verification or monitoring where warranted;
- **High Risk:** EDD, required approval and enhanced ongoing monitoring;
- **High Risk Override:** Mandatory High Risk treatment irrespective of score; and
- **Zero Tolerance:** Rejection, restriction or termination, subject to applicable legal and regulatory requirements.

Detailed operational requirements shall be governed by the Client Acceptance Policy, CDD Procedure and other applicable Company policies and procedures.

9. INDIVIDUAL CLIENT RISK SCORING MODEL

The Individual Client Risk Scoring Model assesses the inherent financial crime risk associated with an Individual Client, subject to the Zero Tolerance and High Risk Override requirements under Section 8.

The model consists of four weighted risk categories:

Risk Category	Weight
Customer / Relationship Risk	30
Product / Transaction / Delivery Risk	30
Geographic Risk	25
Business / Sector Risk	15
Total	**100**

Each factor shall be rated from **0 to 4** and calculated in accordance with the methodology established under Section 8. The aggregate weighted category scores constitute the Individual Inherent Risk Score.

9.1 Customer / Relationship Risk – Weight 30

This category assesses characteristics of the Client and the business relationship that may increase financial crime risk.

Factor	Internal Weight
Client Profile and Transparency	30%
Source of Funds / Source of Wealth Profile	30%
Expected Relationship and Transaction Profile	25%
Adverse Information / Behavioural Indicators	15%
Total	**100%**

Client Profile and Transparency

Rating	Assessment
0	No relevant risk identified
1	Clear and transparent profile with readily verifiable information
2	Minor complexity or limited additional verification required
3	Material complexity, inconsistencies or elevated transparency concerns
4	Significant transparency or profile concerns requiring enhanced scrutiny

Source of Funds / Source of Wealth Profile

Rating	Assessment
0	Not applicable / no relevant risk identified
1	Clear, plausible and readily verifiable SoF/SoW
2	Reasonable SoF/SoW requiring additional supporting information
3	Material complexity or difficulty in verification
4	Significant concerns regarding plausibility or verifiability, without independently triggering a High Risk Override

Where SoF remains materially unexplained or unverifiable after reasonable clarification and verification, the High Risk Override provisions under Section 8 shall apply.

Expected Relationship and Transaction Profile

Rating	Assessment
0	No relevant risk identified
1	Simple and clearly understood expected activity
2	Moderate transaction volume, frequency or complexity
3	Materially elevated volume, frequency or complexity
4	Highly complex or unusual expected activity creating significant inherent financial crime exposure

Adverse Information / Behavioural Indicators

Rating	Assessment
0	No relevant adverse information or behavioural concern
1	Minor information with limited risk relevance
2	Relevant concerns requiring clarification or monitoring
3	Credible and material adverse information or behavioural concerns
4	Serious and credible concerns requiring enhanced scrutiny, without independently triggering an override

9.2 Product / Transaction / Delivery Risk – Weight 30

This category assesses risks arising from the nature, value, frequency, funding and execution of transactions.

Factor	Internal Weight
Transaction Value and Volume	30%
Cash Exposure	25%
Third-Party Payments / Funding	25%
Transaction Complexity and Behaviour	20%
Total	**100%**

Transaction Value and Volume

Rating	Assessment
0	No relevant activity
1	Low and proportionate transaction value and volume
2	Moderate activity consistent with the Client profile
3	High value or volume requiring increased scrutiny
4	Exceptionally high or concentrated activity creating significant inherent risk

Cash Exposure

Rating	Assessment
0	No cash exposure
1	Incidental and low-value cash activity
2	Moderate cash activity
3	Material cash activity or recurring cash transactions
4	Significant cash intensity, unusual frequency or structuring characteristics

Third-Party Payments / Funding

Rating	Assessment
0	No Third-Party payment exposure
1	Limited and transparent Third-Party involvement
2	Occasional Third-Party payments with reasonable economic rationale
3	Material or recurring Third-Party payments requiring enhanced verification
4	Significant or complex Third-Party funding creating substantial inherent risk

Transaction Complexity and Behaviour

Rating	Assessment
0	No relevant risk identified
1	Straightforward activity consistent with the expected profile
2	Moderate complexity or occasional deviation from expected activity
3	Material complexity, unusual patterns or repeated deviations
4	Highly complex or unusual transaction behaviour creating significant inherent financial crime exposure

9.3 Geographic Risk – Weight 25

This category assesses the Client's material geographic exposure, including residence, nationality where relevant, Source of Funds, counterparties and transaction-related jurisdictions.

Factor	Internal Weight
Corruption / Governance Risk	40%
FATF / AML-CFT Jurisdiction Risk	35%
Offshore / Secrecy Exposure	25%
Total	**100%**

Corruption / Governance Risk

Rating	Assessment
0	No material geographic exposure
1	Low corruption / strong governance environment
2	Moderate corruption or governance risk
3	Elevated corruption or governance risk
4	High corruption / weak governance environment

FATF / AML-CFT Jurisdiction Risk

Rating	Assessment
0	No material exposure
1	Jurisdiction with generally strong AML/CFT framework
2	Identified AML/CFT weaknesses not requiring enhanced jurisdictional treatment
3	Material exposure to a jurisdiction subject to increased monitoring or comparable elevated concern
4	Significant exposure to a materially high-risk jurisdiction not independently subject to a prohibition or override

Offshore / Secrecy Exposure

Rating	Assessment
0	No offshore or secrecy-related exposure
1	Transparent jurisdiction with effective information-exchange standards
2	Moderate offshore exposure with satisfactory transparency
3	Material exposure to jurisdictions with elevated secrecy or transparency concerns
4	Significant secrecy-related exposure materially increasing financial crime risk

CAHRA exposure and applicable sanctions prohibitions shall be treated in accordance with Section 8 and shall not be duplicated through quantitative scoring where an override or Zero Tolerance determination already applies.

9.4 Business / Sector Risk – Weight 15

This category assesses the financial crime exposure associated with the Client's occupation, business activities and economic profile.

Factor	Internal Weight
Sector / Occupation Risk	50%
Cash / High-Liquidity Exposure	25%
Business Model Complexity / International Reach	25%
Total	**100%**

Sector / Occupation Risk

Rating	Assessment
0	Not applicable / no relevant risk
1	Low-risk occupation or business activity
2	Moderate inherent sector risk
3	Elevated-risk activity, including material exposure to cash-intensive or higher-risk sectors
4	High inherent financial crime exposure, including significant activity in precious metals, virtual assets, money services or comparable higher-risk sectors

Cash / High-Liquidity Exposure

Rating	Assessment
0	No relevant exposure
1	Limited cash or highly liquid asset exposure
2	Moderate exposure
3	Material exposure
4	Significant dependence on cash or highly liquid and portable stores of value

Business Model Complexity / International Reach

Rating	Assessment
0	Not applicable
1	Simple and predominantly domestic activity
2	Moderate international or operational complexity
3	Significant international activity, intermediaries or business-model complexity
4	Highly complex or multi-jurisdictional business activity creating significant inherent financial crime exposure

This factor shall not duplicate geographic risk already assessed under Section 9.3.

9.5 Calculation of the Individual Inherent Risk Score

Each factor shall be rated from 0 to 4 and weighted in accordance with Sections 9.1–9.4.
The maximum contribution of each category shall be:

Category	Maximum Contribution
Customer / Relationship Risk	30
Product / Transaction / Delivery Risk	30
Geographic Risk	25
Business / Sector Risk	15
Maximum Individual Inherent Risk Score	**100**

The aggregate weighted category score constitutes the Individual Inherent Risk Score.

9.6 Application of Overrides

Zero Tolerance and High Risk Override criteria shall be applied in accordance with Section 8.

Where an override applies, the quantitative score may be retained for analytical and audit purposes but shall not supersede the applicable override outcome.

9.7. Individual Client Mitigating Controls

Following calculation of the Individual Client Inherent Risk Score, eligible mitigating controls may be applied in accordance with Section 8.6 of this Policy.

Mitigating controls shall be directly relevant to the identified risk, demonstrably effective, supported by sufficient evidence and capable of ongoing verification.

For quantitative purposes, the rating of an individual risk factor may be reduced by a maximum of one (1) rating level where an eligible mitigating control directly and effectively reduces that specific risk.

The cumulative quantitative mitigation adjustment shall not exceed fifteen (15) points from the Individual Client Inherent Risk Score.

All mitigating controls and resulting score adjustments shall be documented, supported by evidence and reviewed by the MLRO / Compliance Function.

Mitigating controls shall not override any Zero Tolerance determination, reduce a Client subject to a High Risk Override below High Risk, or compensate for incomplete mandatory CDD or EDD or unresolved material UBO, SoF/SoW, sanctions, PF, provenance or responsible sourcing concerns.

The Individual Client Residual Risk Score shall be determined in accordance with Section 8.6.

9.8. Individual Client Residual Risk Score and Final Classification

The Individual Client Residual Risk Score shall be calculated after application of eligible mitigating controls in accordance with Sections 8.6 and 9.7.

Where neither Zero Tolerance nor a High Risk Override applies, the Final Risk Classification of an Individual Client shall be determined as follows:

Residual Risk Score	Final Risk Classification
0.00 – 34.99	Low Risk
35.00 – 64.99	Medium Risk
65.00 – 100.00	High Risk

Where a High Risk Override applies, the Individual Client shall be classified as High Risk irrespective of the quantitative score.

Where Zero Tolerance applies, the relationship or activity shall not be accepted or continued, subject to applicable legal, regulatory, freezing, reporting or orderly exit requirements.

The Final Risk Classification shall determine the applicable level of due diligence, approval, monitoring and periodic review in accordance with this Policy and the Company's AML/CFT and related compliance framework.

10. CORPORATE CLIENT RISK SCORING MODEL

The Corporate Client Risk Scoring Model assesses the inherent financial crime risk associated with a Corporate Client, subject to the Zero Tolerance and High Risk Override requirements under Section 8.

The model consists of five weighted risk categories:

Risk Category	Weight
Customer / Ownership & Control Risk	25
Product / Transaction / Delivery Risk	25
Geographic Risk	20
Business / Sector Risk	15
Supply Chain / Provenance / Third-Party Risk	15
Total	**100**

Each factor shall be rated from **0 to 4** and calculated in accordance with the methodology established under Section 8. The aggregate weighted category scores constitute the Corporate Inherent Risk Score.

10.1 Customer / Ownership & Control Risk – Weight 25

This category assesses the transparency, ownership, control and financial profile of the Corporate Client.

Factor	Internal Weight
Ownership and UBO Transparency	35%
Legal / Corporate Structure Complexity	25%
Source of Funds / Source of Wealth Profile	25%
Adverse Information / Regulatory History	15%
Total	**100%**

Ownership and UBO Transparency

Rating	Assessment
0	Not applicable / no relevant risk identified
1	Clear and readily verifiable ownership and UBO structure
2	Moderate ownership complexity but satisfactory transparency
3	Material complexity requiring enhanced verification
4	Significant transparency concerns, without independently triggering a High Risk Override or Zero Tolerance criterion

Where the UBO cannot be satisfactorily established after reasonable measures, or intentional concealment is identified, Section 8 shall apply.

Legal / Corporate Structure Complexity

Rating	Assessment
0	Not applicable
1	Simple operating company with transparent structure
2	Moderate corporate complexity with reasonable economic rationale
3	Multi-layered or cross-border structure requiring enhanced understanding
4	Highly complex structure creating significant inherent financial crime risk

Source of Funds / Source of Wealth Profile

Rating	Assessment
0	Not applicable / no relevant risk identified
1	Clear, plausible and readily verifiable SoF/SoW
2	Reasonable SoF/SoW requiring additional supporting information
3	Material complexity or difficulty in verification
4	Significant concerns regarding plausibility or verifiability, without independently triggering a High Risk Override

Adverse Information / Regulatory History

Rating	Assessment
0	No relevant adverse information
1	Minor or historical information with limited relevance
2	Relevant adverse or regulatory information requiring clarification
3	Credible and material adverse information or regulatory concerns
4	Serious and credible adverse or regulatory concerns requiring enhanced scrutiny, without independently triggering an override

10.2 Product / Transaction / Delivery Risk – Weight 25

This category assesses risks arising from the nature, value, frequency, funding and execution of the Corporate Client's transactions.

Factor	Internal Weight
Transaction Value and Volume	30%
Cash Exposure	20%
Third-Party Payments / Funding	25%
Transaction Complexity and Behaviour	25%
Total	**100%**

Transaction Value and Volume

Rating	Assessment
0	No relevant activity
1	Low and proportionate activity
2	Moderate activity consistent with the Client's business profile
3	High value or volume requiring increased scrutiny
4	Exceptionally high or concentrated activity creating significant inherent risk

Cash Exposure

Rating	Assessment
0	No cash exposure
1	Incidental and low-value cash activity
2	Moderate cash activity
3	Material or recurring cash activity
4	Significant cash intensity, unusual frequency or structuring characteristics

Third-Party Payments / Funding

Rating	Assessment
0	No Third-Party payment exposure
1	Limited and transparent Third-Party involvement
2	Occasional Third-Party payments supported by reasonable economic rationale
3	Material or recurring Third-Party payments requiring enhanced verification
4	Significant or complex Third-Party funding creating substantial inherent risk

Transaction Complexity and Behaviour

Rating	Assessment
0	No relevant risk identified
1	Straightforward activity consistent with the expected profile
2	Moderate complexity or occasional deviation from expected activity
3	Material complexity, unusual patterns or repeated deviations
4	Highly complex or unusual transaction behaviour creating significant inherent financial crime exposure

10.3 Geographic Risk – Weight 20

This category assesses material geographic exposure arising from incorporation, operations, ownership, Source of Funds, counterparties and transaction flows.

Factor	Internal Weight
Corruption / Governance Risk	35%
FATF / AML-CFT Jurisdiction Risk	35%
Offshore / Secrecy Exposure	30%
Total	**100%**

Corruption / Governance Risk

Rating	Assessment
0	No material geographic exposure
1	Low corruption / strong governance environment
2	Moderate corruption or governance risk
3	Elevated corruption or governance risk
4	High corruption / weak governance environment

FATF / AML-CFT Jurisdiction Risk

Rating	Assessment
0	No material exposure
1	Jurisdiction with generally strong AML/CFT framework
2	Identified AML/CFT weaknesses not requiring enhanced jurisdictional treatment
3	Material exposure to a jurisdiction subject to increased monitoring or comparable elevated concern
4	Significant exposure to a materially high-risk jurisdiction not independently subject to a prohibition or override

Offshore / Secrecy Exposure

Rating	Assessment
0	No offshore or secrecy-related exposure
1	Transparent jurisdiction with effective information-exchange standards
2	Moderate offshore exposure with satisfactory transparency
3	Material exposure to jurisdictions with elevated secrecy or transparency concerns
4	Significant secrecy-related exposure materially increasing financial crime risk

CAHRA exposure and applicable sanctions restrictions shall be treated in accordance with Section 8 and shall not be duplicated where they already determine an override or Zero Tolerance outcome.

10.4 Business / Sector Risk – Weight 15

This category assesses the inherent financial crime exposure associated with the Corporate Client's sector, business model and activities.

Factor	Internal Weight
Sector Risk	50%
Cash / High-Liquidity Exposure	20%
Business Model Complexity / International Reach	30%
Total	**100%**

Sector Risk

Rating	Assessment
0	Not applicable / no relevant risk
1	Low inherent sector risk
2	Moderate inherent sector risk
3	Elevated-risk sector or activity
4	High inherent financial crime exposure, including significant activity in precious metals, virtual assets, money services or comparable higher-risk sectors

Cash / High-Liquidity Exposure

Rating	Assessment
0	No relevant exposure
1	Limited exposure
2	Moderate exposure
3	Material exposure
4	Significant dependence on cash or highly liquid and portable stores of value

Business Model Complexity / International Reach

Rating	Assessment
0	Not applicable
1	Simple and predominantly domestic operating model
2	Moderate international or operational complexity
3	Significant cross-border activity, intermediaries or operational complexity
4	Highly complex or multi-jurisdictional business model creating significant inherent financial crime exposure

Geographic characteristics already assessed under Section 10.3 shall not be duplicated under this factor.

10.5 Supply Chain / Provenance / Third-Party Risk – Weight 15

This category applies to Corporate Clients where precious metals sourcing, supply chain, provenance, refining, trading or related Third-Party arrangements are relevant to the relationship.

Factor	Internal Weight
Supply Chain Transparency and Traceability	35%
Provenance / Origin Risk	30%
Third-Party / Intermediary Risk	20%
Responsible Sourcing Control Environment	15%
Total	**100%**

Supply Chain Transparency and Traceability

Rating	Assessment
0	Not applicable
1	Clear and well-documented supply chain with strong traceability
2	Moderate complexity with satisfactory supporting documentation
3	Material gaps, complexity or traceability concerns requiring enhanced review
4	Significant supply chain transparency or traceability concerns

Provenance / Origin Risk

Rating	Assessment
0	Not applicable
1	Clearly established and low-risk provenance
2	Moderate provenance risk with satisfactory supporting evidence
3	Material provenance or origin concerns requiring enhanced verification
4	Significant provenance concerns, without independently triggering an override or Zero Tolerance criterion

Third-Party / Intermediary Risk

Rating	Assessment
0	No relevant Third-Party or intermediary involvement
1	Limited and transparent involvement
2	Moderate involvement with reasonable economic rationale
3	Material reliance on Third Parties or intermediaries requiring enhanced due diligence
4	Significant or complex Third-Party involvement creating substantial inherent risk

Responsible Sourcing Control Environment

Rating	Assessment
0	Not applicable
1	Strong and demonstrable responsible sourcing controls
2	Generally adequate controls with limited weaknesses
3	Material weaknesses requiring enhanced oversight
4	Significant weaknesses in the Client's responsible sourcing control environment

Where supply chain or provenance concerns meet the criteria for a High Risk Override or Zero Tolerance determination under Section 8, the applicable override treatment shall prevail.

Detailed supply chain due diligence requirements shall be governed by the Responsible Sourcing and Supply Chain Due Diligence Policy.

10.6 Calculation of the Corporate Inherent Risk Score

Each factor shall be rated from 0 to 4 and weighted in accordance with Sections 10.1–10.5.

The maximum contribution of each category shall be:

Category	Maximum Contribution
Customer / Ownership & Control Risk	25

Category	Maximum Contribution
Product / Transaction / Delivery Risk	25
Geographic Risk	20
Business / Sector Risk	15
Supply Chain / Provenance / Third-Party Risk	15
Maximum Corporate Inherent Risk Score	**100**

The aggregate weighted category score constitutes the **Corporate Inherent Risk Score**.

10.7. Corporate Client Overrides and Mitigating Controls
Zero Tolerance and High Risk Override criteria shall apply independently of the quantitative Corporate Client Risk Score and shall take precedence over the quantitative scoring outcome.

Following calculation of the Corporate Client Inherent Risk Score, eligible mitigating controls may be applied in accordance with Section 8.6 of this Policy.

Mitigating controls shall be directly relevant to the identified risk, demonstrably effective, supported by sufficient evidence and capable of ongoing verification.
For quantitative purposes, the rating of an individual risk factor may be reduced by a maximum of one (1) rating level where an eligible mitigating control directly and effectively reduces that specific risk.

The cumulative quantitative mitigation adjustment shall not exceed fifteen (15) points from the Corporate Client Inherent Risk Score.

All mitigating controls and resulting score adjustments shall be documented, supported by evidence and reviewed by the MLRO / Compliance Function.

Mitigating controls shall not override any Zero Tolerance determination, reduce a Client subject to a High Risk Override below High Risk, or compensate for incomplete mandatory CDD or EDD or unresolved material UBO, SoF/SoW, sanctions, PF, provenance or responsible sourcing concerns.

The Corporate Client Residual Risk Score shall be determined in accordance with Section 8.6.

10.8. Corporate Client Residual Risk Score and Final Classification
The Corporate Client Residual Risk Score shall be calculated after application of eligible mitigating controls in accordance with Sections 8.6 and 10.7.

Where neither Zero Tolerance nor a High Risk Override applies, the Final Risk Classification of a Corporate Client shall be determined as follows:

Residual Risk Score	Final Risk Classification
0.00 – 34.99	Low Risk
35.00 – 64.99	Medium Risk
65.00 – 100.00	High Risk

Where a High Risk Override applies, the Corporate Client shall be classified as High Risk irrespective of the quantitative score.

Where Zero Tolerance applies, the relationship or activity shall not be accepted or continued, subject to applicable legal, regulatory, freezing, reporting or orderly exit requirements.

The Final Risk Classification shall determine the applicable level of due diligence, approval, monitoring and periodic review in accordance with this Policy and the Company's AML/CFT, responsible sourcing and related compliance framework.

11. SOURCE OF FUNDS AND SOURCE OF WEALTH

Source of Funds ("SoF") and Source of Wealth ("SoW") shall be assessed where relevant to the Client's risk profile and in accordance with applicable CDD and EDD requirements.

The purpose of the assessment is to establish reasonable confidence that the Client's funds and, where applicable, overall wealth are legitimate, plausible and consistent with the Client's known profile and expected activity.

The nature and extent of verification shall be proportionate to risk.

11.1 Source of Funds

SoF refers to the origin of the funds used in the business relationship or transaction.

Relevant sources may include:

- Employment or professional income;
- Business income;
- Investment proceeds;
- Sale of assets;
- Inheritance or gifts;
- Financing from legitimate sources; and
- Other documented and economically plausible sources.

Where SoF is materially inconsistent with the Client's profile, cannot be satisfactorily explained or verified, or involves unexplained Third-Party funding, additional information and verification shall be obtained.

Where SoF remains materially unexplained or unverifiable after reasonable measures, the High Risk Override requirements under Section 8 shall apply.

11.2 Source of Wealth

SoW refers to the origin of the Client's overall accumulated wealth and shall be assessed where required by the Client's risk profile, applicable EDD requirements or other relevant circumstances.

Relevant sources may include:

- Business ownership or profits;
- Employment or professional earnings;
- Investments;
- Property or other asset ownership;
- Inheritance;
- Family wealth; and
- Other legitimate and reasonably explainable sources.

The assessment shall consider whether the Client's overall wealth is reasonably consistent with the information available regarding the Client's background, activities and financial profile.

11.3 Risk Treatment

SoF/SoW information shall be considered as an input into the applicable risk assessment under Sections 9 and 10.

Minor documentary deficiencies or explainable inconsistencies shall not automatically result in High Risk classification.

Material concerns shall be escalated where:

- SoF or SoW is inconsistent with the Client's known profile;
- supporting information appears unreliable or contradictory;
- significant Third-Party funding lacks reasonable economic rationale;
- the origin of funds or wealth cannot be satisfactorily established; or
- the circumstances give rise to suspicion of ML/TF/PF or other financial crime.

Where the circumstances give rise to suspicion, the matter shall be separately escalated to the MLRO in accordance with the Suspicious Transaction Reporting Procedure.

Detailed documentary and verification requirements shall be governed by the Customer Due Diligence Procedure and applicable EDD requirements.

12. ULTIMATE BENEFICIAL OWNERSHIP

GoldTakas FZCO shall identify and verify the Ultimate Beneficial Owner (“UBO”) of Corporate Clients in accordance with applicable legal and regulatory requirements and the Customer Due Diligence Procedure.

The ownership and control structure shall be understood to a degree sufficient to identify the natural person(s) who ultimately own or control the Client and to assess relevant financial crime risk.

12.1 Ownership and Control Risk

The risk assessment shall consider, where relevant:

- Ownership transparency;
- Number of ownership layers;
- Use of holding companies or offshore entities;
- Nominee shareholders or directors;
- Trusts, foundations or comparable legal arrangements;
- Cross-border ownership structures;
- Unexplained changes in ownership or control; and
- Other arrangements capable of obscuring ultimate ownership or control.

Complexity alone shall not constitute High Risk where the structure has a legitimate purpose and the UBO can be satisfactorily identified and verified.

12.2 Inability to Establish UBO

Where reasonable measures have been taken but the UBO or ultimate control cannot be satisfactorily established, the matter shall be treated in accordance with the High Risk Override requirements under Section 8.

Where there is evidence of intentional concealment, falsification or deliberate misrepresentation of beneficial ownership or control, the applicable Zero Tolerance provisions under Section 8 shall apply.

Detailed identification, verification and documentary requirements shall be governed by the Customer Due Diligence Procedure.

13. CLIENT ACCEPTANCE AND RISK-BASED DECISIONING

Client acceptance and continuation decisions shall be based on the Final Risk Classification determined under this Policy and shall be implemented in accordance with the Client Acceptance Policy.

As a general principle:

- **Low Risk Clients** may be accepted subject to completion of applicable CDD requirements;
- **Medium Risk Clients** may require additional verification, controls or monitoring proportionate to the identified risks;
- **High Risk Clients** shall be subject to EDD, enhanced monitoring and required approval;
- **High Risk Override cases** shall be treated as High Risk irrespective of the quantitative score; and
- **Zero Tolerance / Prohibited cases** shall not be accepted or continued, subject to applicable legal and regulatory requirements.

A quantitative score shall not override mandatory CDD or EDD requirements, a High Risk Override, Zero Tolerance determination or applicable legal prohibition.

Commercial considerations shall not justify acceptance or continuation of a relationship where mandatory compliance requirements have not been satisfied.

Detailed approval authorities, acceptance conditions, rejection criteria and onboarding requirements shall be governed by the Client Acceptance Policy.

14. ONGOING REVIEW AND REASSESSMENT

Client risk assessments shall remain current throughout the business relationship and shall be reviewed periodically and whenever material changes occur.

The frequency and depth of review shall be proportionate to the Final Risk Classification.

14.1 Periodic Review

Unless a shorter period is required by applicable law, regulation or identified risk:

- **High Risk Clients:** at least annually;
- **Medium Risk Clients:** at least every two years; and
- **Low Risk Clients:** at least every three years.

Periodic review shall consider whether:

- KYC/CDD information remains current;
- ownership and UBO information remains accurate;
- the Client's activities remain consistent with the expected profile;
- SoF/SoW information remains reasonable where relevant;
- geographic, sector or supply chain exposure has materially changed;
- screening results remain satisfactory;
- material adverse information has emerged; and
- the existing Final Risk Classification remains appropriate.

14.2 Trigger Event Reassessment

A Client risk assessment shall be reviewed before the next scheduled review where a material Trigger Event occurs.

Trigger Events may include:

- Material changes in ownership, control or UBO;
- Material changes in business activity, products or transaction profile;
- Significant changes in transaction volume, frequency or behaviour;
- New or materially increased geographic exposure;
- New PEP or sanctions-related information;
- Material adverse media or regulatory developments;
- Unexplained Third-Party payments or funding;
- Material SoF/SoW concerns;
- Significant supply chain, provenance or CAHRA concerns;
- Material inconsistencies in Client information;
- Suspicious or unusual activity relevant to the Client's risk profile; or
- Other information reasonably capable of affecting the Final Risk Classification.

The occurrence of a Trigger Event does not automatically change the Client's risk classification. The relevant information shall be assessed and the classification revised where warranted.

14.3 Reassessment Outcome

Following periodic or Trigger Event review, the Company shall:

- update relevant risk factors;
- recalculate the quantitative score where applicable;
- reassess any High Risk Override or Zero Tolerance criteria;
- review the continued applicability of mitigating controls; and
- determine the revised Final Risk Classification.

Where the risk classification increases, applicable EDD, approval, monitoring and other controls shall be applied without undue delay.

Material reassessments and their outcomes shall be documented.

15. MODEL GOVERNANCE AND CALIBRATION

The risk-rating methodology shall be subject to appropriate governance to ensure that it remains consistent, proportionate and capable of producing reasonable and explainable risk classifications.

The MLRO / Compliance Function shall oversee the methodology and propose material changes for Senior Management approval.

15.1 Model Validation and Recalibration

The quantitative risk-scoring methodology established under this Policy shall be subject to documented validation at least annually and whenever a material change in the Company's business, Client base, products or services, geographic exposure, financial crime risk environment or applicable legal and regulatory requirements may affect the continued appropriateness of the methodology.

The approved methodology comprises:

a. the Individual Client and Corporate Client risk categories, risk factors and applicable weights defined in Sections 9 and 10;
b. the 0–4 factor rating scale and weighted scoring methodology established under this Policy;
c. a maximum Inherent Risk Score of 100;
d. the application of eligible mitigating controls subject to a maximum reduction of one (1) rating level per relevant risk factor and a maximum cumulative quantitative mitigation adjustment of fifteen (15) points;
e. the following Residual Risk Score classification thresholds:

- 0.00–34.99: Low Risk
- 35.00–64.99: Medium Risk
- 65.00–100.00: High Risk

f. the independent application of Zero Tolerance and High Risk Override criteria, which shall take precedence over quantitative scoring outcomes.
The MLRO / Compliance Function shall oversee the validation of the methodology.

Validation shall include, at a minimum:

a. testing representative Individual and Corporate Client scenarios across the full risk spectrum;
b. assessing the consistency and reasonableness of Final Risk Classifications;

c. assessing whether risk factors and their respective weights appropriately reflect the relative significance of the underlying risks;
d. assessing whether the approved classification thresholds produce reasonable and sufficiently differentiated Low, Medium and High Risk outcomes;
e. reviewing the frequency, justification and quantitative effect of mitigating controls, including compliance with the one-level-per-factor mitigation limit and fifteen (15)-point aggregate mitigation cap;
f. assessing the effectiveness and continued appropriateness of Zero Tolerance and High Risk Override criteria;
g. reviewing material manual adjustments, exceptions, recurring misclassifications, scoring anomalies or inconsistent application;
h. reviewing the distribution of Clients across Low, Medium and High Risk classifications solely for the purpose of identifying potential model anomalies and not for achieving any predetermined distribution; and
i. considering new or emerging financial crime risks, typologies and regulatory developments.

Validation shall include testing of representative Individual and Corporate Client cases and, where appropriate, back-testing against actual Client activity, monitoring outcomes, compliance findings and material risk events.
Where validation identifies a material weakness or indicates that the methodology no longer produces reasonable, proportionate or sufficiently differentiated risk outcomes, the MLRO / Compliance Function shall propose appropriate recalibration or amendment in accordance with Section 15.2.

The results of each validation, including the testing performed, identified deficiencies, conclusions reached and any recommended corrective actions, shall be documented and reported to Senior Management.
Validation, testing, recalibration and approval records shall be retained in accordance with the record-retention requirements of this Policy.

15.2 Methodology Changes
Any material change to the approved risk-rating methodology shall be subject to formal change control.

Material methodology changes include, but are not limited to, changes to:

- risk categories;
- risk factor definitions or rating criteria;
- internal factor weights;
- category weights;
- the 0–4 factor rating scale;
- the methodology used to calculate category, Inherent or Residual Risk Scores;
- Low, Medium and High Risk classification thresholds;
- mitigating-control eligibility criteria or quantitative mitigation limits;
- High Risk Override criteria; or
- Zero Tolerance criteria.

Any such change shall be:
a. supported by a documented rationale;
b. tested using representative Individual and Corporate Client scenarios;
c. assessed for its impact on existing risk classifications;

d. reviewed by the MLRO / Compliance Function; and
e. approved by Senior Management before implementation.

Where a methodology change may materially affect existing Client classifications, the MLRO / Compliance Function shall determine, on a risk-based basis, whether affected Clients require immediate reassessment or reassessment within a defined implementation period.

No material methodology change shall be applied retrospectively or operationally before the required testing and approval have been completed.

All methodology changes, testing results, approvals, implementation dates and resulting reassessments shall be documented and retained in accordance with this Policy.

16. INTEGRATION WITH THE AML/CFT FRAMEWORK

This Policy forms an integral part of the GoldTakas FZCO AML/CFT compliance framework and shall not be applied as a standalone risk-management instrument.

The AML/CFT Policy establishes the Company's overarching financial crime compliance framework, while this Policy establishes the methodology for assessing and classifying Client risk.

The resulting Final Risk Classification shall inform the application of:

- Client acceptance requirements;
- CDD and EDD;
- ongoing monitoring;
- periodic review;
- sanctions and PEP-related risk treatment;
- transaction monitoring; and
- responsible sourcing and supply chain due diligence, where applicable.

Information obtained through these controls shall, in turn, be considered in the Client risk assessment where material.

Risk classification and suspicion are separate concepts. A High Risk classification does not, by itself, establish suspicion, and a Low or Medium Risk classification shall not prevent escalation of suspicious activity to the MLRO.

Where another Company policy or procedure imposes a mandatory or more stringent requirement, that requirement shall apply.

17. ROLES AND RESPONSIBILITIES

Responsibilities under this Policy shall be allocated in a manner that supports effective oversight, consistent application and appropriate segregation of duties.

17.1 Senior Management

Senior Management shall be responsible for:

- approving this Policy and any material amendments;
- approving the risk-rating methodology, including material changes to risk categories, factor or category weights, classification thresholds, mitigation limits and override criteria;
- reviewing material findings arising from model validation or recalibration;
- ensuring adequate resources, systems and controls are available to implement and maintain the risk-rating framework; and
- approving High Risk relationships where required under the Company's Client Acceptance and AML/CFT framework.

Senior Management approval shall not override any applicable legal prohibition, Zero Tolerance determination, sanctions requirement or other mandatory regulatory requirement.

17.2 MLRO / Compliance Function

The MLRO / Compliance Function shall be responsible for:

- maintaining and overseeing the approved risk-rating methodology;
- promoting consistent application of risk factors, rating criteria and scoring methodology;
- reviewing material, complex or escalated risk assessments;
- overseeing High Risk Override and Zero Tolerance determinations;
- reviewing and approving the application of mitigating controls and related quantitative adjustments;
- monitoring the effectiveness and consistent application of the methodology;
- coordinating periodic model validation and, where required, recalibration;
- proposing material methodology changes for Senior Management approval;
- monitoring material exceptions, manual adjustments and recurring scoring issues; and
- escalating material deficiencies or weaknesses in the methodology to Senior Management.

17.3 Business and Operations

Relevant Business, Onboarding and Operations personnel shall be responsible for:

- Obtaining complete and accurate Client information;
- Applying approved risk-assessment processes within their assigned responsibilities;
- Identifying material changes in Client circumstances or activity;
- Escalating Red Flags, inconsistencies and material concerns; and
- Complying with applicable risk-based controls and restrictions.

Commercial considerations shall not influence or override Compliance risk determinations.

17.4 Independent Review

The implementation and effectiveness of the risk-rating framework shall be subject to independent review through Internal Control, Internal Audit or another appropriately independent assurance function, on a risk-based basis.

Material findings shall be reported to appropriate management and tracked through remediation.

18. RECORD KEEPING

GoldTakas shall maintain sufficient records to demonstrate the application, operation and outcomes of the risk assessment and scoring methodology established under this Policy.

Records maintained under this Policy shall include, as applicable:

- completed Client risk assessments and risk-scoring records;
- factor ratings, Internal Factor Weights, Category Scores, Inherent Risk Scores, mitigation adjustments, Residual Risk Scores and Final Risk Classifications;
- information and supporting CDD/EDD documentation relied upon in assigning risk-factor ratings and determining the Client's risk classification;
- documented rationale for ratings requiring professional judgement;
- records of Zero Tolerance determinations and High Risk Overrides, including the basis for their application;
- records of mitigating factors applied, including the supporting evidence and resulting quantitative adjustment;
- records of manual adjustments, exceptions, escalations and approvals made in connection with the risk assessment or Final Risk Classification;
- periodic and event-driven risk reassessments, including material changes identified and resulting changes to the Client's risk classification;
- model validation, testing, recalibration and methodology-change records required under Section 15; and
- relevant approvals and supporting records necessary to demonstrate compliance with this Policy.

Records shall be maintained in a manner that enables the Company to reconstruct the basis, calculation and approval of a Client's risk classification and to demonstrate the consistent application of the approved methodology.

Records maintained under this Policy shall be retained for at least five (5) years, or for such longer period as may be required under applicable legal, regulatory or Company requirements.

The broader retention and record-keeping requirements applicable to CDD, EDD, transaction monitoring, screening, regulatory reporting and other AML/CFT records shall remain governed by the Company's AML/CFT framework and the relevant underlying policies and procedures.

19. EXCEPTIONS

Any exception to the standard risk assessment and scoring methodology shall be exceptional, risk-based, fully documented and subject to appropriate approval.

The MLRO / Compliance Function may determine that a case-specific exception is necessary where the strict application of the methodology would produce an outcome that does not appropriately reflect the Client's actual risk profile, provided that the exception is supported by a documented rationale and does not conflict with applicable legal or regulatory requirements.

An exception shall not alter the approved rating scale, scoring formula, Internal Factor Weights, Category Weights, risk classification thresholds, quantitative mitigation limits, Zero Tolerance criteria or High Risk Override criteria established under this Policy.

Any exception affecting the Final Risk Classification shall clearly document:

- the circumstances giving rise to the exception;
- the outcome that would have resulted from the standard methodology;
- the proposed Final Risk Classification;
- the risk-based rationale for the exception;
- any additional controls or monitoring measures applied; and
- the approval obtained.

Any exception resulting in a lower Final Risk Classification than would otherwise apply under the standard methodology shall require prior Senior Management approval.

No exception may:

- override a Zero Tolerance determination;
- reduce a Client subject to a High Risk Override below High Risk;
- waive or circumvent mandatory CDD or EDD requirements;
- permit a relationship prohibited by applicable law, sanctions requirements or the Company's Client Acceptance Policy; or
- be used for the purpose of avoiding an escalation, approval, monitoring or reporting requirement.

All approved exceptions shall be retained as part of the Client's risk assessment record and shall be subject to periodic review by the MLRO / Compliance Function.

20. POLICY REVIEW AND APPROVAL

This Policy shall be reviewed at least annually and earlier where material changes occur in:

- Applicable legal or regulatory requirements;
- The Company's business model, activities or Client profile;
- Financial crime risks or relevant typologies;
- The risk-rating methodology; or
- Findings from regulatory review, Compliance monitoring, Internal Control, audit or independent assurance.

The MLRO / Compliance Function shall be responsible for maintaining the Policy and coordinating its review.

Material amendments to the methodology, including changes to risk categories, weights, classification thresholds, mitigation methodology or override criteria, shall be subject to appropriate testing and Senior Management approval before implementation.

Each approved version of the Policy shall be subject to appropriate version control, including the approval date, effective date and next scheduled review date.

Where applicable law or a binding regulatory requirement changes before this Policy is formally updated, the applicable requirement shall prevail from its effective date.

This Policy shall become effective upon approval by Senior Management or on such later date as specified in the approval record.