

Know Your Customer Policy

| | |
|----------------------|--|
| Date of inception: | 1 December 2022 |
| Review frequency: | Every year |
| Approval date: | 10 February 2025 (Version 2) |
| Policy owner: | Compliance Officer |
| Related document(s): | Anti-Bribery and Anti-Corruption Policy, Anti-Money Laundering Policy, Code of Conduct, Risk Management Policy, Know Your Customer Questionnaire |
| Public document: | Yes |

1. Policy Statement

WMC is committed to conducting business only with legitimate counterparties (i.e., customers, suppliers, funding providers, agents, contractors and other third parties) that uphold ethical and lawful practices, and that share WMC's core values.

WMC will avoid transactions that may be connected to money laundering, terrorism financing, bribery, corruption, fraud, or any other illicit activities, ensuring compliance with regulatory requirements and protecting WMC's reputation.

2. Purpose

This policy aims to prevent WMC from being involved in and/or associated with—intentionally or unintentionally—money laundering activities, terrorist financing activities, bribery and other forms of corruption or fraud. This policy sets out the process and criteria for the acceptance of counterparties with which WMC will do business.

This policy details the counterparty approval process (KYC process), which is an integral process for WMC's risk management framework. The process serves as a concrete safeguard to prevent the approval of counterparties that may present disproportionate risks that cannot be effectively mitigated. This policy, along with the associated KYC Questionnaire, is specifically designed to identify and assess various risk factors associated with potential counterparties, including reputational, environmental, social, governance (ESG), and compliance risks. These assessments contribute to maintaining WMC's commitment to ethical conduct and legal compliance in all business activities. For further details on the management of these risks, please refer to the Risk Management Policy.

3. Scope

This policy is applicable to all of WMC's Personnel, and all counterparties described in this document.

Capitalized terms used herein shall have the meanings ascribed to them in Section 7.

4. Procedures

WMC's KYC process is completed using WMC's Customer Relationship Management (CRM) platform in accordance with the following steps.

4.1 Counterparty Entry

When initial discussions with a counterparty begin, the WMC Lead will create an entry for the counterparty as a lead in WMC's CRM system.

Once discussions progress to a stage where a transaction is likely to occur, the WMC Lead will formally initiate the KYC process within the CRM system.

4.2 KYC Questionnaire

The first formal step in the KYC process is completion of the KYC Questionnaire. The KYC Questionnaire (available in the CRM system) will be sent to the counterparty by the WMC Lead for completion.

Once the KYC Questionnaire is completed and returned to WMC, the WMC Lead will upload the document into the CRM (along with all other documents sent by the counterparty) and will advance the KYC process to the next stage, where such documents will be sent to the Compliance Officer.

4.3 Document Review and Risk Evaluation

Once the KYC request is received by the Compliance Officer, they will perform a thorough review of the completed KYC Questionnaire and associated documents (e.g., corporate registry profile, audited financials). Additionally, the counterparty's information will be assessed using WMC's third-party compliance due diligence tool, which provides insights into key risk factors, including reputation, sanctions, ownership structure, and geographic risk, to ensure a comprehensive evaluation. This review and evaluation will form the basis of the risk assessment of the counterparty and will include consideration of the following:

| Risk Factor | Low Risk | Moderate Risk | High Risk |
|---------------------------------------|---|--|--|
| Geography | Operates (or has bank accounts) in countries with low corruption risk (e.g., as per Transparency International Corruption Perceptions Index). | Operates (or has bank accounts) in countries with medium corruption risk. | Operates (or has bank accounts) in countries with high corruption risk or under international sanctions. |
| Transaction Type | Routine transactions (e.g., standard supply contracts). | Significant financial value or strategic partnerships. | Involves government officials or high-value contracts with non-transparent terms. |
| Reputation & Compliance Framework | No concerns identified in public records; has a robust compliance framework (e.g., policies, processes). | Minor concerns raised but no formal legal or reputational incidents; has basic compliance policies. | History of fraud, corruption, or media-reported controversies; no discernible compliance framework. |
| Ownership Structure & Source of Funds | Ownership is clear (including publicly traded companies), with beneficial owners well-documented; source of funds originating from verifiable and legitimate business activities. | Ownership includes private entities with some opacity or complexity in identifying ultimate beneficial owners; source of funds is unclear but not directly suspicious. | Ownership is opaque (e.g., shell companies, offshore accounts); source of funds raises red flags, such as links to high-risk industries or unexplained wealth. |

As part of this review, the Compliance Officer may require that additional information be collected from the counterparty.

In addition to the above, if the counterparty is of moderate-to-high risk, a sanctions check will also be performed on its affiliated entities and its owners, officers and directors.

There are some risks that may immediately lead to rejecting a counterparty, such as geographical risk (including operating in a sanctioned jurisdiction), appearance on a sanctions list, or if the counterparty is involved in certain high-risk activities (e.g., arms trading or other criminal activity).

4.4 Approval Decision

After completing the risk analysis described in Section 4.3, above, the Compliance Officer will:

- i. If all risk factors fall into the low risk category, approve the counterparty with no conditions;
- ii. If any risk factors fall into the moderate risk category, approve the counterparty only if the Compliance Officer is satisfied that any identified risks have already been sufficiently mitigated;
- iii. If any risk factors fall into the moderate risk category and such risks have not been sufficiently mitigated, conditionally approve the counterparty with additional measures being implemented to mitigate specific identified risks;
- iv. If any risk factors fall into the high risk category or multiple risks fall into the moderate risk category, elevate the approval decision to WMC's Risk Management Committee, unless the Compliance Officer believes such risks have been thoroughly mitigated or additional measures can be implemented to accomplish this; or
- v. Automatically reject the counterparty in the case of certain risks, as further described in Section 4.3, above.

If the approval decision is elevated to WMC's Risk Management Committee, this committee will consider the risks identified by the Compliance Officer and decide if additional information is required or if a third party investigation should be completed into the counterparty. The WMC Risk Management Committee will make the final decision on whether the counterparty will be approved and if any additional measures will be instituted by WMC to mitigate certain risks.

WMC will not enter into any legally binding commitments (except for a non-disclosure agreement) with a counterparty until such time as the counterparty has been approved in accordance with WMC's KYC process.

4.5 Training and Awareness

Training on this policy and its contents is provided to Personnel at the discretion of the Compliance Officer (which will include regular periodic training as well as training upon the occurrence of any significant compliance incidents).

Additional training is available for Personnel upon request.

This policy will be provided to all Personnel through the WMC Intranet.

4.6 Monitoring and Reporting

During the relationship with the counterparty, it is important to revisit the risk profile of the counterparty periodically to ensure all risks are adequately mitigated and that the values of the counterparty and WMC still align. It is possible that the counterparty's risk profile or values have changed, and it is also possible WMC's tolerance of risk or values have changed.

It is anticipated that the Compliance Officer will perform the following actions periodically:

| Action | Period |
|--|---|
| Perform a sanctions check on the counterparty using WMC's third-party compliance due diligence tool. In addition, if any risk factors in Section 4.3 fell into the moderate or high risk categories, also perform a sanctions check on its affiliated entities, its owners, officers and directors. | No less than quarterly |
| Verify bank account details (by phone call). This action will be done by the WMC Lead. | Upon first payment/at time of onboarding and every time a counterparty changes its bank account details |
| Re-evaluate the primary risks for the counterparty and ensure they are adequately mitigated, which could include a re-distribution and completion of the KYC Questionnaire. | Every second year or upon a significant change in circumstances |

When a WMC Personnel discovers that (i) a counterparty has incurred a change in its ownership or management or a significant operational change, (ii) there is a significant change in the values of WMC or the counterparty, such that there is no longer the desired alignment, or (iii) the counterparty has violated applicable laws or is involved in a public controversy, the WMC Personnel must inform the Compliance Officer who will decide on the appropriate measures to take, in consultation with WMC's Risk Management Committee.

This policy is regularly monitored by the Compliance Officer.

Following an incident or complaint, the Compliance Officer will conduct an investigation and provide the WMC board with a report, including findings, recommended actions, and preventative measures to mitigate future risks.

5. Policy Violations

To report non-compliance (or suspected non-compliance) of this policy, please contact the Compliance Officer—who will evaluate what action is required and appropriate.

WMC Personnel who violate this policy, or do not report violations of this policy, will be subject to appropriate disciplinary measures which could include legal action and/or termination of their employment or contract.

6. Other

6.1 Related Information

Additional information regarding WMC's values and guidelines on the acceptable behaviours of its Personnel is provided in further detail in the Code of Conduct.

Information regarding the Anti-Bribery and Anti-Corruption Policy, Anti-Money Laundering Policy, Code of Conduct and Risk Management Policy is available for WMC Personnel on WMC's Intranet.

Questions or comments pertaining to this policy may be directed to the Compliance Officer.

6.2 Policy History

Version 1 Effective 1 December 2022

Version 2 Effective 10 February 2025

7. Definitions

| | |
|--------------|--|
| COUNTERPARTY | Any person or entity that WMC does business with or is considering doing business with, including WMC's (potential) customers, suppliers, funding providers and contractors. |
| KYC PROCESS | WMC's counterparty approval process. |
| PERSONNEL | WMC employees and third parties acting on behalf of WMC. |
| WMC LEAD | The WMC Personnel that will be the person responsible for managing the commercial relationship with the proposed counterparty. |
| WMC | WMC Group B.V. and its affiliates. |