IGC GROUP
THE MAKE MATTERS

Schupstraat 15
2018 Antwerp
Belgium
T +32 3 203 45 67
F +32 3 231 16 34
info@igcgroup.com
www.igcgroup.com

# ANTI-MONEY LAUNDERING

## GROUP POLICIES & PROCEDURES

Anti-Money Laundering, Anti-Terrorism Financing, and Other Financial Crimes

Dr. Anne-Marie De Scheemaecker
November 2017 / Update JUN 2026

SIGHTHOLDER
OF THE DE BEERS GROUP OF COMPANIES

SIGHTHOLDER™ is a trademark used under licence from The De Beers Group of Companies.

RESPONSIBLE JEWELRY COUNCIL
CERTIFIED MEMBER
0000 0549

**Table of Contents** ..... 1

1. Corporate Integrity ..... 2
2. Business Partners ..... 2
3. Trade-Based Money Laundering ..... 2
4. Anti-Money Laundering and Anti-Financial Crime Statement ..... 3
5. Governance Framework ..... 3
6. Policies and Procedures ..... 4
6.1. Bribery and Facilitating Payments ..... 4
6.2. Anti-Money Laundering, Terrorism Financing, and Financial Crimes ..... 5
6.2.1. Identification and Verification: Know Your Customer (KYC) ..... 5
6.2.2. Risk Assessment, Management, and Mitigation ..... 7
6.2.3. AML Risk Analysis ..... 7
6.2.4. Filing of Suspicious Activity and Transaction Reports ..... 12
6.2.5. Training and Awareness Program ..... 13
6.2.6. Audits ..... 14
7. Records ..... 16
7.1. Data Storage ..... 16
7.2. Sustained Vigilance ..... 16
7.3. Updating ..... 16
7.4. Maintenance ..... 17
8. IGC Commitment ..... 17
9. IGC Commitment ..... 17
Appendix A. Legal Cash Limitations ..... 17
Appendix B. Where to Report ..... 20
Appendix C. Definition of Terms ..... 22
Appendix D. AML Seminar Certificate ..... 23
Appendix E. FATF 40+9 recommendations ..... 24

## 1. Corporate Integrity

IGC Group of Companies (IGC) is committed to conduct its operations with honesty, integrity, openness; with respect for the human rights and interests of its employees and their communities; with respect for the environment; and in adherence to the highest ethical standards.

IGC complies with the diamond industry's Best Practice Principles (BPP) through its De Beers Global Sightholder Sales (DBGSS) affiliation as well as the jewelry industry's Code of Practices (COP) through the Certified Membership of the Responsible Jewelry Council (RJC).

The Group Compliance Team is committed to monitor IGC's compliance with the BPP, COP, and all national and applicable international rules and regulations addressing money laundering and other financial crimes.

IGC honors the legitimate interests of all its business partners and is committed to contending dishonesty and fraud in all its transactions so to maintain and enhance consumer trust in, and the reputation of, the diamond and diamond jewelry industries. No practice or conduct will be undertaken nor allowed by any of IGC's managers and employees globally that could bring the diamond or diamond jewelry industry into disrepute. All IGC Member Entities are required to comply with the laws and regulations of the countries in which they operate.

## 2. Business Partners

IGC is dedicated to establishing mutually beneficial relations with its customers, suppliers, and other business partners throughout its global supply chain, and expects its business partners to adhere to business principles that are consistent with theirs. Therefore, IGC will use *Best Endeavors* to ensure the commitment of its diamond suppliers, its diamond customers, and if applicable, its subcontractors to comply with the BPP and COP. IGC is conducting strict and ongoing due diligence on the business relationships and scrutinizes all transactions undertaken throughout the course of that relationship to ensure that the transactions are consistent with IGC's identification and knowledge of the counterparties, as well as their business and risk profile, including the source of funds and destination of goods.

## 3. Trade-Based Money Laundering

Following the high value of diamonds and the easiness of their transportation, the diamond sector is particularly vulnerable to money laundering in the form of disguising

proceeds of crimes by moving the value through trade transactions and as such legitimizing the illicit origin.

## 4. Anti-Money Laundering and Anti-Financial Crime Statement

All Member Entities of the IGC are committed to the highest standards of Anti-Money Laundering (AML) and Anti-Financial Crime (AFC), including but not limited to, Anti-Bribery and Corruption (ABC), Counter-Terrorism Financing (CTF), Anti-Fraud, and other indictable financial crimes, such as smuggling, embezzlement, racketeering, transfer pricing, illegal trade, and tax evasion.

IGC will only conduct business with companies whose business is legal and whose funds come from legitimate sources. Money laundering is facilitated through the use of shell companies, structuring deposits, smurfing, overseas banking, and/or underground banking, and therefore, such means are intensively triggered and investigated.

IGC has its headquarters in Antwerp, Belgium, and is supervised by the Belgian Federal Financial Supervisory Authority under the general AML Law (2017) and Royal Decree (2019) regarding AML for the diamond industry. Belgium is a member country of the Financial Action Task Force (FATF) and the European Union (EU).

IGC has enacted laws and rules at each IGC Member Entity designed to implement the AML policies of global organizations contending money laundering and terrorist financing, including FATF, the U.S. Patriot Act, the Bank Secrecy Act (BSA), and the EU Anti-Money Laundering Directive. The purpose of these laws is to detect, prevent, and report any issue regarding potential money laundering, fraud, terrorist financing, bribery, facilitation, or other financial crimes. IGC Member Entities globally are subject to the same strict due diligence and comprehensive measures. (See Appendix E)

Additionally, as a De Beers Sightholder and RJC Certified Member, IGC is compelled to comply with AML regulations stipulated in the respective BPPs and COPs. IGC strictly adheres to all applicable laws and regulations in all the countries where it conducts business or has a business relationship. IGC examines its AML strategies, purposes, and objectives on an ongoing basis and maintains an effective program for the Group's business that reflects those best practices and principles.

## 5. Governance Framework

The Group Compliance Team consists of the Ultimate AML Responsible, the Operational AML Officer (GOO), the Group KYC Officer (GKO), and local compliance officers.

The GOO has been assigned by the Board of Directors (BOD) with a Group-wide discretionary power over AML-related matters. He/she has unrestricted access to all information, data, records, and systems at all IGC Member Entities considered necessary to fulfill his/her obligations, and reports directly to the BOD.

The GOO is responsible for Group-wide adherence to applicable AML regulations and obligations as well as for establishing and maintaining IGC's AML program to identify, assess, monitor, and manage risks related to money laundering, terrorist financing, and other financial crimes. The GKO is responsible for collecting, verifying, maintaining, and updating the required data from customers and suppliers, an is assisted by the local compliance officers at each Member Entity of IGC Group. Any potential issue or suspicion must be reported to the GOO immediately, who will further assist in investigating the issue and deciding whether reporting to the respective AML Authorities is required.

## 6. Policies and Procedures

IGC has developed a clear set of policies and procedures outlining its general AML standards and principles. Detailed documents and forms are used to ensure that these standards are implemented into day-to-day business practices at each IGC Member Entity worldwide.

The AML policy is published on the company website and in a public folder on the IGC Member's local server, which enables managers and employees to consult it at any time. The AML policy is subject to a bi-annual review and is updated if applicable to ensure conformity with current AML laws and regulations.

### 6.1. Bribery and Facilitating Payments

Each IGC Member Entity will conduct its operations in accordance with the principles of fair competition and all applicable laws and regulations.

Managers and employees may not offer or accept any gift which is, or can be considered as, being a bribe or facilitating payment. The accounting records of the IGC Member Entity and the supporting documents must accurately describe and reflect the nature of the underlying transactions and are subject to regular and independent review.

IGC prohibits bribery in all its business practices carried out on its behalf by its managers, employees, agents, and/or business partners. It is prohibited

- to offer, accept, or condone any payments, gifts in kind, hospitality expenses or promises as such, that may compromise the principles of fair competition or constitute an attempt to obtain or retain business
- to direct business to any person or company to influence the course of any business or governmental decision-making process.

For each Member Entity, IGC requires its managers and employees to report any attempted bribery or facilitating payment to their local compliance officer, who will immediately inform the GOO. Managers and employees will not suffer any adverse consequences or penalties for voicing concerns or reporting attempts of bribery or facilitating payment to the company, its corporate head office, or the authorities.

IGC requires to communicate its Anti-Bribery Policy to all new managers, employees, and counterparties. Suppliers must submit detailed invoices for goods and services purchased by the company before the payment of the invoice is approved. Only invoices that correspond with the delivered goods and services, including the correct amounts and correct prices, will be approved for payment by wire or by cheque.

IGC prohibits hiring managers and employees or entering into a business relationship with new counterparties without the completion of a comprehensive internal risk assessment. IGC prohibits entering or retaining a business relationship with any managers, employees, customers, suppliers, agents, or other business partners who are believed to pose a risk for bribery or facilitating payment.

## 6.2. Anti-Money Laundering, Terrorism Financing, and Financial Crimes

IGC will, at all times, comply with national and relevant international laws and legislations regarding money laundering, terrorism financing, and other financial offences.

IGC has implemented a strict Group-wide KYC program to ensure all customers, suppliers, and other business partners are subject to adequate identification, risk-based assessment, and monitoring measures. The program has been implemented globally at all IGC Member Entities and data are centralized and accessible in the Group's secured CRM platform.

### 6.2.1. Identification and Verification: Know Your Customer (KYC)

- All IGC Member Entities will identify and verify the identity of all their counterparties using reliable, independent source documents, data, and information.
- All counterparties are required to provide proof of incorporation or similar evidence of the legal status of the legal person or organization, as well as information concerning the business partner's name, legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement.
- Any person purporting to act on behalf of the counterparty must validate that he/she is authorized to do so, and the identity of the person must be provided.
- All new customers and suppliers must complete the KYC Form.
- All collected information needs to be verified using reliable sources, including:
    - Belgian Company Registry and UBO Register – for Belgian companies
    - Moody's/Orbis – for non-Belgian companies
- Each IGC Member Entity must take reasonable measures to identify and verify the identity of the Ultimate Beneficial Owner (UBO) of any counterparty, including forming an understanding of the ownership and control structure, such that the IGC Member Entity is satisfied that it knows who the UBO is. The ty.pe of measures needed to satisfactorily perform this function would require the following actions:
    - identification of the UBOs: the natural persons who, whether acting alone or together or through one or more juridical persons, exercise control through 25% or more ownership or voting rights, or who ultimately have a controlling ownership interest.
    - if unable to identify the UBO, identification of the natural persons who comprise the Senior Management of the legal person or organization.
- Where the counterparty is a *Publicly Listed Company* listed on a regulated public stock exchange in the European Economic Area, Australia, Hong Kong or the United States, it is not necessary to seek identification and verification of the identity of any shareholder of that company.

- Depending on the location of the IGC Member Entity, following additional documentation is required:
    - copy of the annual AML report;
    - BPP/RJC declaration completed and signed;
    - U.S. Patriot Act Compliance Form completed and signed.

The IGC Member Entity must conduct ongoing due diligence on their business relationships and scrutinize all transactions undertaken throughout the course of that relationship. Any counterparty with whom no transactions have been conducted over the past 12 months, and with whom a new transaction is presented, will automatically be subject to a fresh and integral KYC identification and verification procedure.

IGC bears the ultimate responsibility for accepting a business partner and conducting a transaction. Therefore, strict and comprehensive due diligence is substantial to protect IGC and its business.

### 6.2.2. Risk Assessment, Management, and Mitigation

Each Member Entity must identify, assess, and prioritize potential risk and undertake the required actions to mitigate, monitor, minimize, and control the probability of money laundering activity. The Group KYC Officer must intensify his/her investigation measures to the degree of perceived risk in situations that seem to bear an increased chance of money laundering or terrorism financing.

In case of any suspicion, he/she must hold the acceptance process and inform the GOO immediately, who will verify and file a Suspicious Activity Report if needed.

### 6.2.3. AML Risk Analysis

IGC has implemented an ongoing AML Risk Analysis process to assess the level of risk exposure presented in the view of the Group's counterparties and/or their geographical location/country, and to develop appropriate security measures from this analysis.

AML safeguards are derived from the results of the AML Risk Analysis. Based on objective risk criteria, counterparties are divided into categories depending on the perceived level of risk:

***Low Risk***

A low risk is considered when:

- the identity and ownership structure are simple and easy to verify
- the business activity is clear and logical
- the transaction fits the counterparty's profile
- there are no links to high-risk countries, PEPs, or negative media

Required Due Diligence: Standard:

- basic identification
- verification
- routine monitoring

***Medium Risk***

A low risk is considered when some risk factors are present but they can be reasonably explained and do not immediately trigger suspicion:

- slightly more complex company structure
- larger or less typical transactions, but still justifiable
- limited connections to higher-risk jurisdictions or sectors

Required Due Diligence: Simplified:

- ask additional questions
- verify certain elements more carefully
- monitor transactions more closely

***High Risk***

A high risk is considered when one or more significant risk indicators are present, or when there is lack of transparency:

- political exposed persons (PEPs)
- links to high-risk or sanctioned countries (*see country risk*)

- use of cash, third party payments or unusual transactions or structures
- complex or unclear ownership structures
- active in sectors other than diamond and diamond jewelry

- frequently changes bank accounts or business trading partners without a plausible explanation
- negative media or reputational concerns

Required Due Diligence: Enhanced (EDD):

- collect additional information and documentation
- verify the source of funds and, where relevant, the source of wealth
- obtain internal approval before proceeding with the transaction or business relationship
- apply increased and ongoing monitoring
- if the risks cannot be sufficiently understood or mitigated, the transaction and the relationship must be refused

***Unacceptable Risk***

An unacceptable risk is considered when:

- a bad experience with the customer, supplier, or business partner has happened
- false or forged information has been provided in the past;
- the counterparty
    - asks to refrain from carrying out an investigation in return for money;
    - is on a terrorist or fugitive suspects list;
    - is on a sanctions or embargo list;
    - was convicted for a serious crime;
    - insists on a transaction in cash

Required Due Diligence: SAR

- end the relationship
- file a SAR

***Country-Risk***

The following countries have been identified by FATF and EU (5th AML Directive) as bearing high AML risk (retrieved from http://www.fatf-gafi.org/countries/#high-risk): [13/02/2026]

A. High risk call for action (blacklist):
High-Risk Jurisdictions subject to a Call for Action - 19 June 2026

- Democratic People's Republic of Korea (DPRK)
- Iran
- Myanmar

B. High risk under increased monitoring (grey list):
Jurisdictions under Increased Monitoring - 19 June 2026

- Angola
- Bolivia
- Bosnia and Herzegovina
- Bulgaria
- Cameroon
- Cote d'Ivoire
- Democratic Republic of Congo
- Haiti
- Iraq
- Kenya
- Kuwait
- Lao People's Democratic Republic
- Lebanon
- Monaco
- Nepal
- Papua New Guinea
- South Sudan
- Syria
- Venezuela
- Vietnam
- Virgin Islands (UK)
- Yemen

#### 6.2.3.1. Management and Control

The IGC AML program is formulated and globally directed by the GOO and addresses all AML-related topics. For all these topics, IGC has developed and implemented a comprehensive set of measures to identify, manage, and control potential risks, which must be complied with globally by all IGC Member Entity managers and employees. The IGC internal organization enables each Member Entity to centralize and communicate information to detect, mitigate, and inhibit

transactions related to money laundering, terrorism financing, and other financial crimes.

In each IGC Member Entity, the Compliance Officer must ensure compliance within his/her Entity with the following obligations:

- ensure that the Entity complies with obligations drafted under the Anti-Money Laundering policy
- ensure that the Entity complies with the applicable *cash limitations* (see Appendix A)
- ensure to provide a written or electronic Annual Activity Report
- act as a *bonus pater familias.*

#### 6.2.3.2. Customer Acceptance Policy (CAP)

Each IGC Member Entity applies a counterparty acceptance policy, allowing to investigate in advance the risk of money laundering or terrorist financing associated with the profile of the client and with the nature of the business relationship or the desired transaction. No transaction can take place without the prior formal approval by the GKO or GOO, or a member of the IGC Member Entity's BOD.

The General Principles of the CAP are the following:

- the GKO must classify customers, supplier, and business partners into the various risk categories as described in §6.2.2.1., and decide on the acceptance criteria for each category based on the risk perception.

- where the customer, supplier, or business partner is a prospect, the account will be opened only after the relevant due diligence and identification measures and procedures have been conducted, the Customer/Supplier Verification Form has been completed, the required documentation and signed documents have been collected, and the account has been approved by the GKO, GOO, or the BOD.

#### 6.2.3.3. Prohibited Business Relationships

The IGC Member Entity must refuse any business transaction or enter into a business relationship if the compliance team is not convinced that it knows the true identity of the business partner, its UBO, and/or the nature of the business; or

if the formal requirements concerning the identification of the customer/supplier and/or its UBOs are not met. The compliance team must intensify its investigation measures to the degree of perceived risk as described in §6.2.2.1.

#### 6.2.3.4. Group-Wide Controls

Adherence to the Group-wide AML program is audited by the GOO on a regular basis (minimum once per year) for each IGC Member Entity, to ensure that IGC's efforts are successful. The compliance team is therefore obliged to implement and conduct appropriate customer and supplier-related controls in order to ensure that all applicable AML requirements are being adhered to and that security measures are properly functioning. The GOO and GKO further ensure that controls are comparable and equally comprehensive across all IGC Member Entities.

#### 6.2.3.5. Sanctions and Embargo Regulations

IGC ensures to comply with all embargo regulations globally as required through the Bank Secrecy Act. IGC is considering the potential risks in designing, implementing and testing its anti-money laundering and trade embargo compliance program.

AWDC has developed a Sanctions & Embargoes Compliance Guide for the Diamond Industry which is available at https://www.awdc.be/sanctions-and-embargoes

### 6.2.4. Filing of Suspicious Activity and Transaction Reports (SARs)

If a transaction or business relationship seems unusual, inconsistent, or suspicious - even without proof of wrongdoing – it must be stopped and immediately reported to the relevant authority:

- **before** the transaction is carried out , indicating the expected timing of the transaction.
- **immediately after** (if reporting beforehand was not possible), clearly explaining why prior notification was not possible**.**

Reporting suspicious activity is important, because it helps to:

- detect and prevent money laundering and terrorist financing
- protect your business from legal and reputational risks
- contribute to the integrity and transparency of the diamond sector

A SAR report must be filed by the GOO when:

- the risk assessment identifies at least one unacceptable risk, or
- multiple risk factors make it unsafe to proceed

Examples of risk factors for filing a SAR:

- the source of funds is unclear or cannot be verified: for example, the counterparty cannot explain where the money comes from or provides inconsistent information.
- the transaction does not make economic or logical sense: for example, buying or selling diamonds without a clear business reason.
- the counterparty is unwilling to provide information or documents: lack of transparency is a strong risk indicator.
- there are signs of structuring or attempts to bypass legal limits: for example, splitting cash payments to stay below the legal threshold.
- unusual payment methods, such as third-party payments without a clear justification
- the counterparty is linked to criminal activity, sanctions, or negative media, including fraud, corruption, tax evasion, or other illegal activities
- suspicion of or use of false or forged documents
- the transaction involves high-risk countries without a clear explanation
- the counterparty insists on secrecy or unusual confidentiality
- in the event an employee discovers an unusual or suspicious transaction which involves a member of IGC's management, the employee must immediately report the transaction to the GOO and/or the BOD

The diamond trader (or any employee) who submits a report is protected by the authorities against threats or acts of aggression, when he/she is good faith SAR reports are confidential and not shared with third parties.

### 6.2.5. Training and Awareness Program

Across the Group, IGC has implemented an AML education and training program to ensure that all relevant managers and employees undergo a

comprehensive education and training. This training program is based on the guidance received from AWDC and tailored to the diamond and diamond jewelry business, so to ensure that managers and employees are aware of the various potential patterns and techniques of money laundering and financial crime that may occur in their daily business operations.

Training covers the general obligations arising from applicable, legal, and regulatory requirements as well as internal policies, procedures, and communication means. It further includes the resulting discrete duties which must be adhered to in everyday business as well as typologies to recognize money laundering or financial crime activities and transactions.

Regular AML training at each IGC Member Entity globally is provided by the GOO to ensure that all relevant managers and employees are reminded of their duty to timely notify any suspicious activity. In case it would occur, the necessary steps will then be taken to file a SAR report.

#### 6.2.5.1. Reliability and Obligations of Managers and Employees

IGC Group applies hiring policies that help to ensure that only reliable managers and employees are employed. Each member of IGC's compliance team has the professional experience, due diligence, hierarchical level, and authority needed to exercise his/her function.

Managers and employees will be liable for the failure to report information or suspicion regarding money laundering or terrorist financing to the compliance team. Managers and employees must cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is a slight suspicion that they are related to money laundering or terrorist financing.

### 6.2.6. Audits

Both internal and external third-party audits are organized on a regular basis at each of the IGC Member Entities to verify compliance with the AML laws and regulations.

#### 6.2.6.1. Internal AML Audit

The GOO will perform an internal audit at least once per year at each of the IGC Member Entities to review and evaluate the appropriateness, effectiveness, and adequacy of the policy, practices, measures, procedures, and control mechanisms

applied for the prevention of money laundering and terrorist financing. The local compliance officer will perform an internal audit at a regular basis to verify compliance with the AML requirements. The internal audit comprises of:

- a random sample of sales and purchase invoices from the previous calendar year, including at least five domestic and, if applicable, five international transactions;
- verification of the payment records and bank statements of the invoices paid for conformity with AML requirements;
- verification of the customer/supplier KYC records, based on the IGC Member Entity local requirements, laws, and regulations;
- in the case of nonconformance or remarks, a full review of all accounts is performed;
- provision of internal audit report

#### 6.2.6.2. External AML Audit

As a De Beers Sightholder, IGC is required to adhere to De Beers' BPPs, including AML practices. Through an independent and internationally qualified auditor (SGS), De Beers performs:

- annual desktop reviews for each Member Entity based on completed workbooks on the BPP online SMART platform;

- regular on-site audits at each of the Member Entities based on the IGC Member Tier and the De Beers selection

For those Member Entities that are RJC Certified Members, i.e. IGC Group NV, IGC New York, SSL, VDC and ZDL, as well as IGC Jewelry and Diamonds (non-Member Entity and business partner), a three-yearly on-site audit is organized by RJC through an independent and internationally qualified auditor.

Depending on the national laws and regulations at the location of the IGC Member Entity, on-site AML audits are performed by the national government authorities on an ad hoc basis.

#### 6.2.6.3. Financial Accounts Audit

IGC maintains financial records of all its business transactions, which are annually and independently reviewed and certified by a knowledgeable,

independent financial auditor. The auditor is appointment without bias or influence.

Each Entity of the IGC Group will act in accordance with national laws and regulations regarding the auditing of its financial accounts and will have its financial accounts independently audited on an annual basis.

## 7. Records

All IGC Member Entities will keep records on the identification data obtained through the due diligence process, account files, and business correspondence for at least five years after the business relationship ended.

### 7.1. Data Storage

All IGC Member Entities will retain all necessary records on transactions, both domestic and international, as well as the AML Activity Reports for at least ten years, in a secured location to enable IGC to comply swiftly with information requests from the relevant authorities. Data storage is done in compliance with the GDPR regulations and access is restricted to a limited number of authorized persons.

### 7.2. Sustained Vigilance

Every IGC Member Entity must remain alert at all times and persistently examine all transactions and facts where money laundering or terrorism financing is suspected and draw a written report of the examination.

### 7.3. Updating

For all active counterparties, the collected identification data are updated according to the level of the perceived risk.

Any counterparty with whom no transactions have been conducted over the past 12 months will be subject to a fresh and integral identification and verification process at the time a new transaction would emerge.

To stay updated with the AML obligations, the GOO and GKO will pass the annual online AML quiz or 3-yearly physical AML exam.

### 7.4. Maintenance

All IGC Member Entities will, for at least ten years, retain all necessary records on transactions, both domestic and international, in a secured location to enable IGC to comply swiftly with information requests from the competent authorities.

## 8. IGC Commitment and Implementation

An organization's AML controls can be easily undermined by a poor culture of compliance. Therefore, IGC supports and maintains a strong AML culture throughout all its Member Entities, enabling them to prevent shortcomings, identify issues before they become a concern, and result in more efficient AML solutions.

Every Director and Manager within IGC is firmly committed to enforce the principles and the policies described above, and compliance with these principles is considered an essential element of IGC's global success and reputation.

The AML efforts are integrated with a sound understanding across the IGC Member Entities worldwide, allowing them to identify and address potential risks in a fast and efficient manner. To achieve the desired goals, the necessary human, financial, and technical resources are made available Group-wide. Resources are regularly reviewed against IGC's size, complexity, and exposure to risk.

Because it is important that all managers and employees understand the *what* and *why* of compliance with regard to the activities they undertake, the compliance team continuously undertakes the necessary training and actions to build awareness of IGC's AML culture and policies throughout the organization.

IGC is incorporating effective AML controls into its business processes in a way that compliance becomes an integrated part of its daily business practices. Annual internal and external audits enable monitoring the effectiveness of IGC's commitment to help contending money laundering, terrorism financing, and other financial crimes.

## 9. IGC Contact Information

Ultimate AML Responsible: Kirill Van den Abbeele, KVA@igcgroup.com
Operational AML Officer: Anne-Marie De Scheemaecker, ADS@igcgroup.com
Group KYC Officer, Sipaskasina Theeravittayaparn (Tina), STH@igcgroup.com
Group Compliance Officer: Phimtarwat Narunthorn (Phim): PNA@igcgroup.com
Local Compliance Officer New York: Laurie Thompson: LTH@igcgroup.com

## Appendix A. Legal Cash Limitations

*Updated: April 2026.*

**BELGIUM** (IGC ANTWERP)

Cash limit of maximum 3,000 €

A maximum of 10% of the transaction price (the amount on the invoice) or the service can be paid in cash. This limitation includes pre-payments and partial payments, and no cash transaction may exceed 3,000 euro.

Dealing in cash above this threshold is considered a criminal offense and fines for illegitimate use of cash may be very high.

The cash law of the country in which of with whom the deal is done, applies.

**USA** (IGCNY– IGCJD)

Federal law requires a person to report cash transactions of more than $10,000 by filing IRS Form 8300, Report of Cash Payments over $10,000 received in a trade or business.
Form 8300 is required for businesses as well as individuals who engage in a transaction that results in the transfer of cash as follows:

- over $10,000
- received as:
  - a lump sum over $10k
  - two or more related payments in excess of $10k (combined)
  - payments received as part of a single transaction (or two or more related transactions) that exceed $10k in a 12-month period.
- received in the course of trade or business
- from the same person (payer)
- received in a single transaction or two or more related transactions.

**HONG KONG** (IGCHK – IGCJS)

Cash payments in Hong Kong are widely accepted but subject to regulations regarding large amounts and specific merchant limitations. Travelers must declare physical currency exceeding HK$120,000, while daily cash payments at post offices for government bills are limited to under HK$120,000. Retail cash payments, particularly for amounts over HK$5,000 at convenience stores, may face restrictions.

**CHINA** (IGC SH)

While China is effectively a "cashless society" where mobile payments (Alipay/WeChat Pay) dominate over 80% of transactions, cash remains legal tender. However, there are significant practical, legal, and regulatory limitations on its use.
New 2026 Regulations:
Effective February 1, 2026, new rules require all in-person service providers to support cash, specifically targeting "QR-code-only" policies and ensuring self-service machines have cash alternatives.
Travelers can carry up to RMB 20,000 or foreign currency equivalent to USD 5,000 in or out of China without declaration

**THAILAND** (SSL)

Cash payment limitations in Thailand are primarily governed by anti-money laundering regulations, with stricter reporting requirements for large transactions and specific rules for cross-border currency movement.
As of March/April 2026, financial institutions require customers withdrawing 5 million baht or more in cash to explain the source and purpose of the funds to combat "gray" capital and money laundering.
Incoming transactions over 50,000 baht may be subject to stricter reporting to anti-money laundering authorities.
Travelers may bring foreign currency equivalent to USD 20,000 or less without declaration. If more than USD 20,000 (or equivalent), it must be declared to Customs.

**LAO PDR** (VDC)

Cash payment limitations in Laos are primarily driven by low ATM withdrawal caps, a scarcity of high-denomination banknotes, and strict foreign exchange regulations. While there is no specific, universally enforced law prohibiting large cash payments, practical limitations exist due to the physical volume of cash and banking restrictions

**BOTSWANA** (ZDL)

Travelers entering or leaving Botswana with cash (Pula or foreign currency) equivalent to or exceeding 10,000 Pula must declare it to customs. Failure to do so may lead to prosecution.
Financial institutions are required to report large cash transactions. Transactions involving P10,000 or more often require filling out forms to record details of the customer and the transaction for AML purposes.
Business Payment Constraints: While cash is still widely used in the informal sector, there is a push to move to electronic payments. Large-value payments (typically over P500,000) are generally expected to be processed through electronic means (BISS) rather than cheques or cash.

## Appendix B. Where to Report

**BELGIUM (**IGC ANTWERP**)**

*The Belgian Financial Intelligence Processing Unit* (CFI)
Tel: +32-2.533.72.11
e-mail: info@ctif-cfi.be
website: https://www.ctif-cfi.be/

**USA** (IGC NY– IGC BS)

*U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN")*
Helpline: +1-800-949-2732
e-mail: FRC@fincen.gov
website: https://www.fincen.gov/

**HONG KONG** (IGC HK – IGC JS)

*Joint Financial Intelligence Unit (JFIU)*
Tel: 852) 2866 3366
e-mail: jfiu@police.gov.hk
website: www.jfiu.gov.hk

**CHINA** (IGC SH)

*China Anti-Money Laundering Monitoring & Analysis Centre (CAMLMAC)*
*Address: Block A, International Enterprise Building, 35 Financial Street, Xicheng District, Beijing, China*
Website: www.camlmac.pbc.gov.cn

**THAILAND** (SSL)

*Anti-Money Laundering Office (AMLO)*
422 Phaya Thai Rd,
Wang Mai, Pathum Wan,
Bangkok 10330
Phone +66 0 2280 2080
Email info@amlo.go.th

**LAO PDR** (VDC)

*Anti Money Laundering Intelligence Office (AMLIO)*
T4 Road, Phonthan Village,
Saysettha District,
Vientiane, Lao PDR.
Phone: +856 21 264624
e-mail: amlio@bol.gov.la

**BOTSWANA** (ZDL)

*Financial Intelligence Agency (FIA)*
Private Bag 0190
Gaborone, Botswana
Tel: +267 3998400
Email: bpsoko@gov.bw

## Appendix C. Definition of Terms

*Anti-Money Laundering (AML):* AML laws are designed to prevent illegal funds (such as funds obtained from crime, corruption, and tax evasion) from entering the financial system. Financial institutions are required to have procedures in place (such as KYC) to discover high-risk clients, monitor transactions and report suspicious activities (FAFT).

*Bribe:* A bribe is an illegal payment given or promised in order to induce or influence the judgment or conduct of a person in a position of trust.

*Due diligence:* Due diligence is a critical element of effectively managing the organizations risks and protecting it against potential financial crimes and nefarious activities. There are two steps in due diligence: (a) understanding the customer activities and (b) assessing the money laundering risk. When onboarding a new customer or if the customer activities substantially change, an analysis of the source of funds and risk associated with those funds is prudent and, in most countries, a legal requirement

*Facilitating Payment*: A financial payment that may constitute a bribe and that is made with the intention of expediting an administrative process. A facilitating payment is a payment made that acts as incentive to complete some action or process expeditiously, to the benefit of the party making the payment.

*Know Your Customer (KYC):* KYC is a legal requirement to perform identity checks and do customer due diligence. While KYC laws differ from country to country, the general principle involves collecting enough information to properly identify an individual and ensure that their activities are legitimate (FAFT).

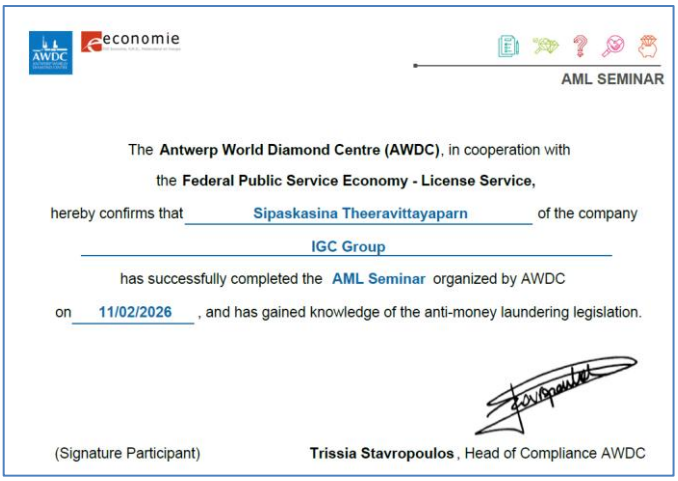
*Ultimate Beneficiary Owner (UBO):* the UBO of a company refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.” That is to say, you need to know who you are doing business with, the real person (or group of people) who owns or controls that business (FAFT).

## Appendix D. AML Seminar Attendance Certificate

AML SEMIN

The **Antwerp World Diamond Centre (AWDC)**, in cooperation with
the **Federal Public Service Economy - License Service,**
hereby confirms that **Anne-Marie De Scheemaecker** of the company
**IGC Group**
has successfully completed the **AML Seminar** organized by AWDC
on **03/12/2025**, and has gained knowledge of the anti-money laundering legislation.

(Signature Participant) **Trissia Stavropoulos**, Head of Compliance AWDC



AML SEMINAR

The **Antwerp World Diamond Centre (AWDC)**, in cooperation with
the **Federal Public Service Economy - License Service,**
hereby confirms that **Sipaskasina Theeravittayaparn** of the company
**IGC Group**
has successfully completed the **AML Seminar** organized by AWDC
on **11/02/2026**, and has gained knowledge of the anti-money laundering legislation.

(Signature Participant) **Trissia Stavropoulos**, Head of Compliance AWDC

**ANTI-MONEY LAUNDERING SEMINAR**

The **Antwerp World Diamond Centre (AWDC),** in cooperation with the
**Federal Public Service Economy - License Service,** hereby confirms
that **PHIMTARWAT NARUNTHORN** of the company

IGC GROUP NV has successfully
completed the **Anti-Money Laundering Seminar** organized by AWDC
on 27 JANUARY 2026, and has gained knowledge of the anti-money laundering legislation.

(Signature Participant) Karen Rentmeesters, CEO AWDC

## Appendix E. FATF 40+9 Recommendations

## FATF 40 Recommendations

*1-10: Legislative and Institutional Framework*

1. Risk-Based Approach : Countries should adopt a risk-based approach to anti-money laundering (AML) and counter-terrorist financing (CFT).
2. National Cooperation and Coordination : Governments must ensure coordination and cooperation among relevant authorities.
3. Money Laundering Offense : Criminalization of money laundering based on a comprehensive legal framework is necessary.
4. Confiscation and Provisional Measures : Implement measures to locate, seize, and confiscate proceeds of crime.
5. Terrorist Financing Offense : Criminalize the financing of terrorism in national legislation.
6. Financial Institution Secrecy Laws : Laws should facilitate effective implementation of AML/CFT measures.
7. Customer Due Diligence (CDD) : Financial institutions must perform due diligence on customers and business relationships.
8. Politically Exposed Persons (PEPs) : Apply enhanced scrutiny on PEPs and their associates.
9. Third-Party Reliance : Define conditions under which institutions can rely on third parties for CDD.
10. Record Keeping : Maintain records of transactions and customer identification for a specified period.

*11-20: Reporting and Monitoring*

11. Reporting Suspicious Transactions : Institutions must report transactions suspected of being linked to money laundering or terrorism.
12. DNFBPs : Ensure that Designated Non-Financial Businesses and Professions (DNFBPs) are subject to AML/CFT measures.
13. Regulation and Supervision : Authorities should effectively regulate and supervise financial institutions and DNFBPs.
14. Guidance and Feedback : Provide guidance and feedback to institutions to enhance compliance.
15. Verification of Identity : Strict identity verification processes should be in place for all clients.

16. Monitoring of Transactions : Continuously monitor transactions for unusual or suspicious activity.
17. Information Exchange : Enhance cooperation and information exchange among competent authorities.
18. International Cooperation : Promote international collaboration in AML/CFT efforts.
19. Mutual Evaluations : Ensure countries participate in regular evaluations of their compliance with FATF Standards.
20. Risk Assessment : Governments must assess and understand the money laundering and terrorist financing risks they face.

*21-30: Sector-Specific Measures*

21. Money Remittance Services : Establish effective regulations for money remitters.
22. Financial Institutions : Ensure robust measures are in place for banks and other financial institutions.
23. Securities Markets : Implement effective measures for exchanges and securities dealers.
24. Life Insurance : Apply anti-money laundering measures to the life insurance sector.
25. Casinos : Ensure casinos implement strict AML/CFT measures.
26. Trade-Based Money Laundering : Address risks associated with trade-based money laundering.
27. Cross-Border Cash Controls : Implement effective controls on cross-border movements of cash.
28. Wire Transfers : Ensure that wire transfers include accurate sender information.
29. Non-Financial Businesses : Extend AML/CFT measures to non-financial sectors.
30. Compliance Programs : Mandate compliance programs in relevant sectors.

*31-40: Special Measures and International Standards*

31. Risk-Based Approach : Implement a risk-based approach regarding vigilant measures.
32. Implementation of SRs : Countries should enforce Special Recommendations addressing terrorism financing.
33. Training and Awareness : Raise awareness and provide training on AML/CFT for all relevant sectors.
34. Effective Laws and Regulations : Ensure that legal frameworks are effective, flexible, and enforceable.

35. Investigative Powers : Give law enforcement agencies adequate powers for investigations.
36. Effective Sanctions : Establish appropriate sanctions for non-compliance.
37. Public Awareness : Promote public awareness about the risks of money laundering and terrorist financing.
38. Whistleblower Protection : Provide protection for individuals who report suspicious activities.
39. Use of Technology : Encourage the use of technology to combat money laundering and terrorist financing.
40. Regular Review and Improvement : Continually review and improve AML/CFT efforts based on emerging threats.

**The 9 Special Recommendations (SR)**

1. SRI : Criminalize the financing of terrorism.
2. SRII : Freeze and confiscate terrorist assets.
3. SRIII : Report suspicious transactions related to terrorism.
4. SRIV : Implement measures to report and prevent terrorist financing through non-profit organizations.
5. SRV : Prevent the abuse of charities and non-profit organizations for terrorist financing.
6. SROI : Ensure measures are in place to combat terrorist financing from both domestic and foreign sources.
7. SRVII : Make financial institutions aware of potential terrorist financing risks.
8. SRVIII : Promote inter-agency cooperation on combating terrorist financing.
9. SRIX : Improve international cooperation in addressing the threats of terrorist financing.

These recommendations provide a comprehensive framework for countries to develop or improve their policies and legal frameworks related to AML/CFT. They are periodically updated, reflecting changes in financial and socio-economic landscapes. For specific implementations or compliance details, countries may refer to their national guidelines based on these FATF recommendations.