Compliance Week AML Syllabus 2026

April 20 - 24, 2026

AWDC

Table of Contents

Introduction 3

Chapter One: AML in the Antwerp Diamond Industry 4

Chapter Two: Legal Obligations within the AML Legislation 10

Chapter Three: Know Your Counterparty (Client or Supplier) 16

Chapter Four: Risk Assessment and High-Risk Situations 24

Chapter Five: Reporting Specific Activity 45

Chapter Six: How to Prepare for an AML Control 51

Chapter Seven: AML Templates, Tools and Manuals offered by AWDC 56

Glossary 62

Annex 69

Introduction

Anti-money laundering (AML) is a key topic for companies in the diamond sector. The Belgian government strictly monitors compliance with AML legislation and places great importance on knowledge of and adherence to these rules within the sector.

As a sector federation, AWDC aims to support and guide Antwerp diamond companies as effectively as possible in achieving efficient and correct compliance with the applicable regulations. With this syllabus, we aim to translate the often complex AML legislation into day-to-day practice and provide the necessary knowledge in an accessible way.

Starting in 2026, the Belgian government will organize a large-scale in-person AML exam for the first time. The purpose of this syllabus is to optimally prepare diamond companies for this. At the end of each chapter, you can test your knowledge using sample questions based on input from the Federal Public Service Economy (FPS Economy) and representative of possible exam questions.

We wish you good luck and an enjoyable learning experience!

Chapter One: AML in the Antwerp Diamond Industry

What can I find in this chapter?

1.1 What is AML?

1.2 Who is subject to the AML legislation

1.3 Why is it important to be AML compliant?

1.4 What does an AML journey look like within a diamond company?

1.1 What is AML?

Anti-Money Laundering (AML) legislation - referred to as antiwitwas (AWW) wetgeving in Dutch - aims to prevent money laundering and the financing of terrorism. In the case of money laundering, the objective is to conceal the illegal **origin** of funds, whereas in terrorism financing, the goal is to conceal their illegal **destination**.

AML consists of a set of legal rules and procedures that require diamond companies (as well as other regulated entities and sectors such as financial institutions, real estate agents, professional football clubs, etc.) to detect and report suspicious financial flows.

Anti-money laundering legislation is not new; it has been in force for many years. With the law of 12 januari 2004, the diamond sector was officially brought under preventive anti-money laundering obligations. Beyond the legal framework and obligations, AML has become an integral part of modern business operations, helping companies mitigate certain risks. Moreover, AML legislation is not only applied in Belgium but is implemented across major financial markets worldwide.

Three organisations play an important role in AML for diamond companies in Belgium:

- FPS Economy — inspects diamond companies and checks whether AML rules are followed
- AWDC — supports diamond companies with practical tools, templates, and training
- CFI — receives and analyses reports of suspicious transactions

The current AML framework consists of:

- AML Law (2017) — the general Belgian law on money laundering
  - Updated by the Royal Decree of 17 March 2024
- Royal Decree (2019) — specific AML rules for the diamond sector

The diamond sector is particlularly vulnerable to money laundering due to characteristics such as:

- High value and small size of diamonds: they are valuable goods that can be transported very easily and discreetly.
- **International and opaque nature:** the trade is highly international. Many diamond companies operate through international structures, with subsidiaries in multiple countries and free trade zones (such as Dubai), where oversight may sometimes be limited.

- Despite increasingly strict regulations, some parts of the value chain outside Antwerp still rely on informal trading practices and cash payments, which makes monitoring more difficult.

→ This makes diamonds attractive to individuals with criminal or illegal intentions as a means to conceal or move financial flows.

1.2 Who is subject to the AML legislation?

- All traders in diamonds and/or synthetic diamonds,
- brokers and producers who use diamonds and/or synthetic diamonds in the manufacture of equipment,
- self-employed persons and companies, governed by either Belgian or foreign law, provided that they have a branch or subsidiary in Belgium.

1.3 Why is it important to be AML compliant?

<u>For your company</u>

As a diamond trader, you are legally required to comply with AML regulations.

- In case of violations, administrative €250 and €1,250,000 may be imposed.
  - The fines are imposed by the FPS Economy and collected by the FPS Finance.
- You also risk reputational damage and the loss of business partners if you fail to comply with the legislation.
- You might, unconsciously, be helping terrorist organizations (something you do not want to do).

<u>For the Antwerp diamond sector</u>

Compliance by each individual company has a direct impact on the entire sector. Every five years, the Financial Action Task Force (FATF) evaluates how vulnerable a country is to money laundering.

A poor FATF report leads to:

- Stricter regulations and increased government controls
- Reduced trust from banks
- Reduced trust from mining companies and international clients (such as jewelry brands

Strong compliance, on the other hand, results in:

- Greater trust from banks and financial institutions
- Greater trust from international partners
- A strong reputation for Antwerp as the world's most trusted diamond trading center

1.4 What does an AML journey look like within a diamond company?

Before entering in a new business relationship or transaction, you must follow a set of mandatory steps.

Together, these steps form the **AML journey**, which applies to every client, supplier, and transaction. Above 10.000 euros or more than one transaction under 10k.

Step 1: Organisational obligations

Before entering into a business relationship with a potential client or supplier, you as a registered diamond company must comply with a number of legal and organisational obligations:

- Have an internal AML policy;
- Appoint at least one AML officer;
- Follow the AML webinar every year or pass the AML exam, which from 2026 onwards will be organised by the government every three years;
- Submit an annual AML report to the authorities.

Step 2: KYC (Know Your Counterparty)

Once your company complies with all organisational obligations, you are ready to enter into your first business relationship with a client or supplier.

However, before you actually do business, you **must collect all AML-related information** about your counterparty, **verify** its accuracy, and ensure it is **kept up to date.**

This process is called **KYC (Know Your Counterparty)**. In short: always know who you are doing business with, before you start doing business.

Step 3: Risk analysis

Based on the information you have gathered about your counterparty during the KYC process, you must carry out a **risk analysis** in which you **assess how safe or risky it is to do business** with this party.

You can conduct this risk analysis manually by using risk scorecards or digitally via the KYCP platform. During this process, you **assign a risk category** to your counterparty (low, medium, or high), and ensure this **information is continuously kept up to date**. If relevant changes occur, such as changes in the counterparty's shareholder structure, the risk analysis must be performed again.

Step 4: Decide on proceeding with the business relation (or not)

The outcome of the risk analysis shows whether it is safe and legally allowed to do business. Based on this, you decide whether to accept the relationship, accept it under certain conditions, or refuse or terminate it.

Step 5: Reporting suspicious situations

During the entire AML process, suspicious situations may arise, for example, a client insisting on paying large amounts in cash, wanting to proceed quickly and skip the KYC process, or a **counterparty providing incomplete, contradictory, or clearly incorrect information** about their identity, their company, or the ultimate beneficial owners of the company ("UBO").

As soon as something appears unusual or suspicious, you must report it to the Financial Intelligence Processing Unit (CFI), even if you do not have concrete or tangible proof of fraud or money laundering and it is only a suspicion.

Practical example:

You are a diamond trader in Antwerp and you are contacted by a new international client based outside Europe. He shows interest in a batch of diamonds and wants to move quickly. At first glance, everything seems attractive, until he mentions that he wants to pay for the goods in **cash**.

At that moment, your AML journey begins. You cannot simply accept the deal, no matter how attractive it may seem. First, you need to know **who you are dealing with**. You **gather information** about the client (= KYC process): who is it, which company does he represent, and where does the money come from? **You verify the information** and check whether everything is accurate.

Next, you conduct a **risk analysis**: you will check whether it is safe and legally allowed to do business with this party. An international client based outside Europe who wants to move quickly and wants to pay in cash for high-value diamonds: these are **clear risk factors**. You assess these elements and determine whether the risk is low, medium, or high. Here we are in a **high-risk situation**.

Based on this, you make a decision: do you proceed with the deal, impose additional conditions (for example, no cash payment), or refuse the transaction altogether? If something does not add up or the risk is too high, you must not only stop the process but also **report it to the Financial Intelligence Processing Unit**.

This is what AML looks like in practice: not a theoretical exercise, but a series of deliberate steps you take to protect yourself, your company, and the entire Antwerp diamond sector.

Test Your Knowledge

(correct answers are provided at the end of this syllabus)

1. What is the maximum amount of the fine for a legal entity under Belgian anti-money laundering legislation in case of non-compliance by a diamond trader?
    a. 1.000.000 euro
    b. 2.000.000 euro
    c. 3.000.000 euro
    d. 1.250.000 euro

2. Which Belgian government service is responsible for conducting AML inspections?
    a. FPS Finance
    b. CFI
    c. FPS Economy

Chapter Two: Legal Obligations for Diamond Companies under AML Legislation

What can I find in this chapter?

2.1 What are the legal obligations for diamond companies under the AML legislation?

2.1 What are the legal obligations for diamond companies under the AML legislation?

Anti-money laundering (AML) legislation imposes a wide range of obligations on diamond companies. As a diamond trader, you are legally required to take effective measures to prevent money laundering and terrorist financing.

As a diamond company, you have four key legal obligations under AML law. Each one is mandatory.

1. Have a written AML policy
2. Appoint one or multiple AML officers
3. Pass the AML exam every three years, or complete the AML webinar every year
4. Submit an annual AML report to the FPS Economy

In the next sub-chapters, we focus specifically on these **organizational obligations,** in other words, how your company should be structured and managed to ensure full AML compliance.

2.1.1 Have an internal AML policy (mandatory)

Every diamond company must have a robust and **written internal AML policy.**

This policy explains how your own company complies with AML obligations and must be **adapted to your specific business activities**.

At a minimum, the AML policy must include:

- Procedures on **how you identify and verify** your clients and suppliers (KYC)
- Procedures on how you conduct **risk assessments**
- Procedures on how you **keep your AML data up to date**
- Procedures on how you **report suspicious activity** to the CFI
- The names of the **persons being responsible for (being compliant with) AML** in your company (AML officers)
- Procedures for **record-keeping and documentation requirements**

Attention

The policy must be kept up to date and available during AML inspections.

AWDC provides a template that is approved by the FPS Economy and that companies can adapt to their own situation. We recommend all Belgian diamond companies to make use of this template:

2.1.2 Appoint an AML officer (mandatory)

Every diamond company must appoint at least one AML officer: One AML officer at the management level and optionally an extra one at the performance level. There are two roles:

1. T**he ultimate AML responsible** is a person at **senior management level** who ensures the company follows AML law. If you are self-employed, you personally hold this role. The ultimate AML-responsible is required.

2. The **operational AML officer** is appointed by the senior management. This person **handles AML in day-to-day operations**. They ensure AML rules are followed, check risks, monitor counterparties, train staff, and report suspicious activity. If you are self-employed, you also hold this role. The operational AML officer is optional.

The operational AML officer is responsible for:

- Following AML legislation
- Carrying out KYC and risk assessments
- Monitoring business relationships
- Reporting suspicious activity to the CFI
- Training staff on AML
- Getting an AML certificate each year (webinar) or every three years (exam)
- Writing and maintaining the company's AML policy
- Submitting the annual AML report

Attention

During an inspection, it must be immediately clear who the ultimate AML responsible is and who takes the role of operational AML officer.

AML officers must be officially registered with the FPS Economy through the notification of the names of the AML officers on the annual AML report.

It is good practice to formally record the appointment of AML officers in the minutes of a board meeting. Being officially registered is also required to take part in the in-person AML exam.

2.1.3 Take the 3-yearly AML exam or attend the AML webinar every year (mandatory)

To prove that there is sufficient knowledge on AML legislation within your company, an **AML certificate must be obtained by at least one of the official AML officers**.

There are two ways to do this:

- **Participate in and pass the large-scale, in-person AML exam**, organized once every ,three years by the FPS Economy. More information: www.awdc.be/aml-exam.
- **Attend the AML webinar each year**, followed by successfully completing the related questionnaire, via www.MyAWDC.be.

In both cases, you will receive an **AML certificate** upon passing the exam or the questionnaire following the webinar.

Attention

The AML certificate is an important and mandatory part of your annual AML report (See chapter 2.1.4 - Submit your Annual AML Report to the FPS Economy).

Keep the certificate at your company's premises. You must be able to show it during an AML inspection.

Each company must ensure that at least one of its AML officers obtains an AML certificate, either by completing the AML webinar or by passing the AML exam.

2.1.4 Submit your annual AML report with the FPS Economy (mandatory)

Every year, you must submit an AML report covering the previous year to the FPS Economy here:

The report covers:

- Your company's identity
- Your AML organisation and procedures
- How you applied KYC and risk assessments
- Any suspicious activity you reported to the CFI
- How you comply with sanctions rules

Attention

The ultimate deadline for submitting this AML Report is **March 31** (every year).

Only (one of) the AML officer(s) is authorized to prepare, sign and submit the annual AML report.

This manual, guides you step-by-step through the AML report-submission process:

Test Your Knowledge

(correct answers are provided at the end of this syllabus)

1. What is the deadline for submitting the annual AML report?
    a. 1 April
    b. 31 March
    c. 31 May
    d. 1 June

2. How often must you attend an AML training if you have not passed the AML exam?
    a. Every year
    b. Every two years
    c. Every three years
    d. Every four years

3. An AML officer can independently decide to use company resources to meet AML obligations.
    a. True
    b. False

4. Only the AML officer (or the person appointed by management) can prepare the annual AML report.
    a. True
    b. False

5. Which Belgian government body monitors EU financial sanctions?

6. How many times per year must you attend an AML training if you have not passed the exam? (Enter a number)

Chapter Three: Know Your Counterparty (KYC)

What can I find in this chapter?

3.1 What is KYC and AML data collection and why is it important?

3.2 Collecting and verifying AML data

3.3 Updating and maintaining AML data

3.4 GDPR considerations and non-compliance

3.5 Ongoing vigilance during the business relationship

3.1 What is KYC and AML data collection and why is it important?

The purpose of Know Your Counterparty (KYC) is to prevent money laundering and terrorist financing by **understanding who your counterparties are**. KYC ensures that your business does not facilitate illegal activities without knowing.

KYC — Know Your Counterparty — means **collecting and verifying information** about the people and companies you do business with, **before you start working with them**.

The goal is simple: know who you are doing business with.

KYC allows you to:

- Confirm who your client or supplier really is
- Assess how risky it is to work with them
- Detect unusual or suspicious behaviour
- Have the information you need if you ever have to report to the CFI

3.2 Collecting and verifying AML data

3.2.1 When and from whom to collect and verify AML data

You must collect KYC information in the following situations:

- Before starting any business relationship — with a new client or supplier
- OR Before a one-off transaction of €10,000 or more — even if there is no ongoing relationship

If the first transaction with a new counterparty is below €10,000, KYC is not required — unless a second related transaction follows, or unless the counterparty is high risk (for example, a PEP or someone from a high-risk country).

You are responsible for ensuring that counterparty information is accurate, up to date and complete, and that it remains as such during the business relationship. Information should be updated at least annually for high-risk counterparties, and every 2-3 years for low-risk counterparties (infra).

3.2.2 What are the identification requirements?

For a person (individual):

- Full name
- Date and place of birth
- Address (if possible)
- Copy of a valid ID (passport or identity card)

For a company:

- Company name and legal form (e.g. NV, BV, Ltd)
- Registered address
- List of directors
- Ultimate Beneficial Owners (UBOs) — see section 3.2.2.1

3.2.2.1 Identification of Ultimate Beneficial Owners (UBOs)

UBOs are the natural (real) persons who ultimately own or control the company (not just the legal owner on paper) and they are essential for detecting hidden ownership and potential fraud or money laundering.

Attention

You must identify the UBO(s) of every company you do business with.

A person is a UBO if they:

- Own 25% or more of the company's shares or voting rights, or
- Control the company in another way (for example, through a chain of companies)

How to find UBO information:

- For Belgian companies: check the Belgian UBO Register at financien.belgium.be
- For foreign companies: use international databases such as Moody's (available through KYCP), or ask your counterparty directly

If the information you find is incomplete or unclear, it is your responsibility to ask your counterparty for the correct information and verify it using a reliable source.

3.2.3 How to obtain and verify AML information

To obtain AML information, request your counterparty to complete a **Client Information Form** (example forms are available on the AWDC website).

If the counterparty is a Publicly Listed Company (a company that has its shares listed and actively traded on a regulated public stock exchange) in the European Economic Area, Australia, Hong Kong, or the United States, you can identify listed companies in a simplified manner, for example, through the listed company's website. The UBO's of a listed company do not need to be identified.

3.2.4 Verify the information using reliable source

Collecting information is not enough — you must also check that it is correct.This is the required verification process.

Use independent and reliable sources to verify what your counterparty has told you:

- Belgian Company Registry (KBO) — for Belgian companies
- Belgian UBO Register — for UBO information
- KYCP (Moody's / ORBIS) — for international company data

Attention

If identity documents do not look genuine, or company data does not match official registries, do not proceed.

If you find a difference between the UBO information in the Belgian UBO register and the information you collected, you must report this to the register without delay (in any case, within 14 calendar days of their detection).

3.3 Updating and maintaining AML data

KYC information must stay accurate throughout the entire business relationship.

Update your information:

- At least every year — for high-risk counterparties
- Every 2 to 3 years — for low-risk counterparties
- Immediately — when something significant changes (for example, new ownership, new UBOs, negative news)

Updating procedure:

- Send the existing AML file to the counterparty.
- Request written confirmation that the information remains accurate.
- Update the information if necessary.

Attention

Your AML policy should clearly outline the frequency and method of updating counterparty information. You must continuously monitor transactions and behavior to ensure they remain consistent with the counterparty profile.

Maintain your AML data:

AML records must be kept for 10 years after the end of the business relationship or the date of an occasional transaction.

Attention

During this period, all documents must be readily available for the FPS Economy upon request (during an AML inspection, for example).

After 10 years, you are legally required to permanently delete or anonymise all personal data — identification documents, client forms, UBO information, and risk assessments — unless there is a specific legal reason to retain them (such as an ongoing investigation or a formal request from authorities).

When deleting: digital files must be permanently removed from systems and backups; paper files must be shredded.

Keep an internal deletion log recording the counterparty reference, deletion date, and method — but no personal data.

3.4 GDPR considerations and non-compliance

AML obligations are based on a legal requirement, which means you are permitted to collect and process personal data without your counterparty's consent. When AML rules and GDPR rules point in different directions, AML rules win.

You must inform counterparties that their data is being collected. Your counterparties must be informed about:

- The purpose (AML compliance)
- The retention period of the AML information (10 years)
- The fact that this information will possible be shared with authorities

Only collect what is necessary. During the retention period, counterparties cannot demand deletion or object to processing.

Refusal of information providing or identification is not possible

If a counterparty refuses to provide information or identify their UBOs: do not start or continue the relationship, document the refusal, and treat it as a high-risk indicator. If you suspect money laundering (even if you cannot prove it), report to the CFI (see chapter 5 – Reporting Suspicious Activity).

If identification is simply not possible despite reasonable efforts: same outcome — do not proceed, document your steps, and consider a CFI report.

3.5 Ongoing vigilance during the business relationship

KYC does not end when a relationship begins. Updating frequency depends on the risk profile of the counterparty (See chapter 3.3 - Update and maintain your AML data).

Throughout the relationship you must:

- Keep counterparty information up to date (annually for high-risk; every 2–3 years for low/medium risk — and immediately when something significant changes)
- Monitor transactions to ensure they remain consistent with the counterparty's profile and the nature of the relationship
- Stay alert to high-risk signals: repeated cash payment requests, negative media, changes in ownership, ...

If a transaction seems unusual — complex, unusually large, lacking a clear business reason — investigate it, including the origin of funds if needed, and document your analysis in writing. If you cannot satisfactorily explain it, you must:

- Consider suspending or terminating the business relationship;
- Assess whether there is a suspicion of money laundering or terrorist financing and, if necessary,
- **Report to the CFI (See chapter 5 - Reporting Suspicious Activity)**

Do the KYC-Check:

- Know who is your counterparty is
- Know who owns the counterparty, who the UBOs are
- Verify the data you collected
- Update the KYC information on a regular basis
- Delete all personal data 10 years after the end of the business relationship
- Not able to identify your counterparty? Do not start/do not proceed (and consider reporting to the CFI)

Test Your Knowledge

(correct answers are provided at the end of this syllabus)

1. A client refuses to provide an identity document or disclose the names of the UBOs. What do you do?
    a. Continue the relationship, document the refusal, and adjust your risk assessment
    b. Respect the client's privacy and continue the relationship
    c. Refuse the relationship or transaction. If money laundering is suspected, report to the CFI
    d. Continue the relationship but report to the federal judicial police

2. After a business relationship ends, how long must records be kept?

3. Your search finds no information about a counterparty. What do you do?
    a. Treat the counterparty as low risk
    b. Treat as neutral risk and document the search attempt
    c. Do not proceed — you cannot meet your identification obligation
    d. Continue without further verification

4. What steps must a diamond trader follow to identify UBOs of a foreign company?
    a. Ask the company or representative to sign a declaration
    b. Take reasonable steps to collect and verify information (name, address, directors, UBOs) and keep the documents
    c. Only collect director information if the risk is high
    d. Collect only name and address — asking for more violates GDPR

5. KYC data should be updated every year for high-risk clients, and every 2 to 3 years for other clients.
    a. True
    b. False

6. What minimum ownership percentage qualifies someone as a UBO in Belgium?

Chapter Four: Risk Assessment and High-Risk Situations

What can I find in this chapter?

4.1 What is a risk assessment and why should you conduct it?

4.2 When must you conduct a risk assessment?

4.3 What information do you need to conduct a proper risk assessment?

4.4 Categories of risks to consider

4.5 Risk classification: low, medium and high

4.6 Outcome of your risk assessment: accept or refuse?

This chapter is organized into in two parts:

Part A: Theory. What is a risk assessment, how and when should you do it and how do you classify risks?

Part B: High-risk situations in practice: how to apply the theory in the most common high-risk scenarios you will encounter.

PART 1: THEORY

4.1 What is a risk assessment and why is it important?

A risk assessment is a key step in preventing money laundering and terrorist financing.

Before doing business, you must **evaluate the risk of working** with a counterparty (client or supplier) and you should repeat this at several key moments during the business relationship.

You ask yourself one fundamental question: **How risky is it to do business with this person or company?**

The answer to this question will be clear after you did a risk assessment.

A risk assessment follows a risk-based approach. This means that not every counterparty gets the same level of checks. Instead, you adjust your scrunity to the level of risk:

- **Low-risk** counterparties require standard checks
- **High-risk** counterparties require extra checks (called Enhanced Due Diligence or EDD)

The purpose of a risk assessment is to:

- **Know and verify who you are dealing with** (identify your counterparty): KYC (See chapter 3 – Know Your Counterparty)
- Understand **where their money comes from**
- Detect **unusual or suspicious situations**
- Decide whether you can safely **start or continue a business relationship**

Recognizing **high-risk situations** is an essential part of this process. These are situations where the risk of money laundering or fraud is higher, and where additional checks (also called Enhanced Due Diligence (EDD)) are required.

4.2 When must you conduct a risk assessment

4.2.1 Risk assessment of your own company

Before any business is done, you must make an overall analysis of the **AML risks in your own company**.

By understanding your own risks, you can put the right controls in place and avoid being unknowingly involved in money laundering or sanctions breaches.

Use the risk scorecard in Annex A of this syllabus to assess your company's AML risk profile manually, or use the KYCP Portal to perform the assessment digitally.

4.2.2 Risk assessment of your counterparty

A risk assessment of your counterparty must be conducted at several key moments before AND during your business activities. **It is not limited to the start of a relationship** but applies throughout the entire lifecycle of your interaction with a counterparty.

- Before starting a **business relationship**

Is it safe and appropriate to start working with this person or company?

- Before a **one-off transaction**

Even if there is no ongoing relationship, you must still assess the risks associated with the transaction and the counterparty involved.

- When something **significantly changes (in the relationship)**

Like new ultimate beneficial owners (UBO's), new owners, changes in the client's business activities, or any other relevant developments that may impact the risk profile, you must reassess the risk.

- When a **transaction looks unusual**

Transactions that are unusually large, complex, or lack a clear economic purpose.

- As part of a regular **periodic review (ongoing monitoring)**

Client files and risk profiles should be reviewed and kept up to date throughout the relationship. The frequency of reviewing depends on the risk profile (high, medium, low) of the counterparty.

Attention
A risk assessment is never a one-time exercise. You must reassess whenever the circumstances change.

4.3 What information do you need to conduct aproper risk assessment?

To assess the risk properly, you need to understand five things about your counterparty and the transaction:

- **Understand the purpose of the business relationship or transaction**

This means identifying why the client wants to do business with you? What will they buy or sell?

Example
A jeweler wants to buy polished diamonds for resale in their store → logical.
A construction company wants to buy high-value diamonds → unusual and requires further investigation.

- **Understand the scale of the expected business will be**

This means that you know what the expected value of transactions is, how frequently transactions will take place, and what the expected volume of diamonds to be traded is.

Example
A new client immediately wants to buy €2 million worth of diamonds in one transaction, while having no visible track record → higher risk.
A long-term client buying smaller, regular parcels → lower risk.

- **Determine the source of funds**

You understand where the money used in the transaction comes from. Is its origin legitimate and can you verify it?

Example
Payment comes from a well-known company account that matches the client's business activity → low concern.
Payment comes from a private account or an unrelated third party → red flag.

- **Determine the destination of funds**

You know where the money or diamonds are going, and whether this destination is logical and legitimate within the context of the transaction.

Example

A diamond wholesaler buying rough diamonds → consistent.
An individual with no clear business activity trading large volumes of diamonds → unusual and higher risk.

- **Assess the counterparty's business activity or profession**

You should verify whether the counterparty's activities are consistent with the intended transaction or relationship.

To understand what types of risks could be associated with your counterparty, you can use the risk scorecard in Annex B or make use of the GRID screening tool available through the KYCP platform (see chapter 7 – AML Templates, Tools and Manuals).

Attention

The result of the risk screening will impact the final decision to onboard or reject the counterparty. The risk scorecard as well as the risk screening results received via the KYCP support the trader in making this decision (see below, chapter 4.7 - Outcome: Accept or Refuse?)

4.4 Categories of risks to consider

There is no official or exhaustive list of risks to consider when conducting a risk assessment. You must always apply your own professional judgment, based on the specific situation and the information available.

However, **four categories of risk** can help you structure your assessment. If one or more of the questions below can be answered with "yes," this may indicate a higher-risk situation, requiring additional checks.

1. **Counterparty Risk** – related to the characteristics, background, and behaviour of your counterparty:
    - Is your counterparty **a PEP (Politically Exposed Person)?**
    - Is the counterparty **linked to negative news or media?**
    - Is the counterparty **unable or unwilling to explain the purpose of the transaction or business relationship?**
    - Has the counterparty experienced **bankruptcies or financial difficulties** in the past?
    - **Does the company have a complex or unclear ownership structure (UBOs)?**

2. **Geographical Risk -** related to the country or region where your **counterparty** or transaction is linked to:
    - Is the counterparty or transaction **linked to a high-risk country?**
    - Is the counterparty or transaction **linked to a sanctioned country or jurisdiction?**

3. **Transaction Risk –** related to the nature and characteristics of the transaction itself:
    - Is the **transaction unusually large** or does it **not match the counterparty's profile or business activity?**
    - Does the counterpartywant to **pay in cash?**
    - Does the counterparty want to **pay through a third party?**
    - Does the counterparty insist on **unusual or complex payment methods?**

4. **Product/Sector Risk** – related to the inherent characteristics of the goods being traded and the nature of the diamond sector:
    - Does the transaction **involve high-value diamonds?**
    - **Are the goods easily transportable?** Diamonds are small and easy to move, making them more vulnerable to smuggling and illicit trade.
    - **Does the transaction or trade structure lack clear economic logic?**

Attention

These four categories mirror the risk scorecard in Annex B. Work through each category systematically for every new counterparty and whenever your assessment needs to be updated.

4.5 Risk classification: low, medium and high

After collecting all relevant information and identifying potential risk factors, you can **assign a risk level** to your counterparty. This is called **risk classification**.

In practice, counterparties are typically classified as **low, medium, or high risk**.

Risk Level	Characteristics	Due Diligence Required
🟢 LOW	Clear identity, simple structure, no red flags, consistent transactions	Standard due diligence: basic ID, verification, routine monitoring
🟡 MEDIUM	Some risk factors present but can be explained; slightly complex structure	Simplified Due Diligence: additional questions, closer attention, more monitoring
🔴 HIGH	One or more significant risk indicators, or lack of transparency	Enhanced Due Diligence (EDD): extra info, source of funds, management approval, increased monitoring

Risk level: Low Risk

A counterparty is considered **low risk** when there are no significant risk indicators and the situation is clear, transparent, and consistent.

This means:

- 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

For low-risk clients, you apply **standard due diligence**. This includes basic identification, verification, and routine monitoring.

Risk level: Medium Risk

A counterparty is considered **medium risk** when some risk factors are present, but they can be reasonably explained and do not immediately raise suspicion.

This may include:

- A slightly more complex company structure
- Transactions that are larger or less typical, but still justifiable
- Limited connections to higher-risk jurisdictions or sectors

For medium-risk counterparties, you should apply Simplified Due Diligence: ask additional questions, verify certeain elements more carefully, and monitor transactions more closely.

Risk level: High Risk

A counterparty is considered **high risk** when one or more significant risk indicators are present, or when there is a lack of transparency.

Examples:

- Politically Exposed Persons (PEPs)
- Links to high-risk or sanctioned countries
- Use of cash, third-party payments, or unusual transaction structures
- Complex or unclear ownership structures
- Negative media or reputational concerns

For high-risk counterparties, you must apply Enhanced Due Diligence (EDD). This includes:

- Collect additional information and documentation
- Verifying the source of funds and, where relevant, source of wealth
- Obtaining internal approval before proceeding with the transaction or business relationship
- Applying increased and ongoing monitoring
- If the risks cannot be sufficiently understood or mitigated, you must refuse the business relationship or transaction.

4.6 Outcome of your risk assessment: accept or refuse?

After completing a risk assessment, you must decide how to proceed with the counterparty. The decision depends on the level of risk identified and the measures you can take to mitigate it.

The three possible decisions are:

Decision	When	What to do
✅ ACCEPT	Risk is low or manageable	Proceed with standard monitoring and regular due diligence
⚠️ ACCEPT WITH CONDITIONS	Risk is medium or can be reduced	Apply Enhanced Due Diligence (EDD); get management approval before proceeding
🚫 REFUSE	Risk is too high or red flags cannot be explained	Do not proceed. Report to the CFI if you suspect money laundering

Attention

- You must justify your decision for accepting, accepting with conditions, or refusing a counterparty.
- Every decision must be clearly documented, including the information reviewed, risk factors considered, and the reasoning behind your choice.

AWDC offers a ready-to-use KYC and Risk Assessment Conclusion template to help you document your decision consistently:

AWDC offers a ready-to-use KYC and Risk Assessment Conclusion template to help you document your decision consistently:

4.6.1 Documentation and record-keeping

Every risk assessment and related decision must be recorded so that it can be reviewed and audited. Keep a record of:

- Risk level assigned — low, medium, or high
- Key findings — information and observations that informed your assessment
- Decision and reasoning — what you decided (acceptance, acceptance with conditions or refusal) and why
- Supporting documents — ID copies, contracts, emails, screening results

Attention

All records must be organized and retrievable. Make sure this information is available upon request, for example during AML inspections.

PART 2: HIGH-RISK SITUATIONS IN PRACTICE AND HOW TO REACT

The sections below cover the five high-risk situations you are most likely to encounter as a diamond trader. Each section follows the same structure:

- What it is (the theory)
- Why it matters for AML
- What you must do
- A practical example

4.6.2 Politically Exposed Persons (PEPs)

What is a PEP?

A Politically Exposed Person (PEP) is someone who holds — or has held — a prominent public position. The category includes:

- Heads of state or government, ministers, and senior politicians
- Judges of high courts and senior military officials
- Executives of state-owned enterprises
- Immediate family members (spouse, children, parents)
- Close associates (known business partners, close connections)

Attention

A person remains a PEP during their function and for at least 12 months after leaving the position — and sometimes longer, depending on the overall risk assessment.

Why does PEP status matter for AML?

PEPs are considered higher risk because:

- They may have access to public funds
- They can be more exposed to corruption or bribery
- There is a higher risk of money laundering linked to abuse of power

Attention

Being a PEP does NOT mean the person is doing anything illegal. It simply means extra caution is required. You can still do business with a PEP — but only after completing Enhanced Due Diligence (EDD).

What must you do when you identify a PEP?

- **Obtain additional information**, like the source of wealth (how they became wealthy), the source of funds (origin of the money used in the transaction) and the purpose of the business relationship
- **Perform deeper verification**: use reliable and independent sources, check media and public information, screen against sanctions and watchlists
- **Obtain senior management approval before doing business with a PEP**. A PEP relationship cannot be accepted at operational level alone
- **Increase monitoring**: conduct more frequent reviews of the relationship, closer monitor the transactions

Check for PEP status using KYCP (which gives access to GRID), Google, official government websites, and public registers.

- You can check if a counterparty is a PEP using the KYCP platform (which offers you access to GRID, a comprehensive screening and monitoring database), Google searches, official government websites, public registers,...
- PEP status is a **risk trigger**, not a prohibition. You can still do business with a PEP, but only if you: fully understand the origin of their funds, apply enhanced checks, closely monitor the relationship.

Example
You are contacted by a new client who is a retired government minister from an African country. He wants to buy a parcel of high-value polished diamonds.

Step 1 — Identify: During KYC, you discover his former ministerial role. He is a PEP.
Step 2 — Collect extra information: Ask where the money comes from (source of funds) and how he built his wealth (source of wealth).
Step 3 — Verify: Cross-check his information against GRID (for sanctions and PEP databases), public media, and official registers.
Step 4 — Approval: Before proceeding, escalate to senior management for formal sign-off.
Step 5 — Monitor: If accepted, monitor the relationship more frequently than for a standard counterparty.

If you cannot satisfactorily verify the source of funds or wealth, you must refuse and — if you suspect money laundering — report to the CFI.

4.6.3 Engaging with a counterparty located in a 'high risk' country

A high-risk country is a country with an increased risk of money laundering or terrorist financing, for example due to weak controls or high levels of corruption.

Counterparties linked to such countries are automatically considered **higher risk**. This means you must apply Enhanced Due Diligence (EDD) before starting or continuing the business relationship.

There are different lists of countries (black and grey list), published by the FATF, that show **strategic deficiencies in their AML frameworks at various levels**, meaning that doing business with companies established in these countries is either **prohibited** or requires Enhanced Due Diligence (EDD).

The black list

Countries on the **high-risk ("black") list** include:

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

The FATF calls for the application of Enhanced Due Diligence (EDD) measures and, where appropriate, the implementation of countermeasures. These measures may vary from one country to another.

The Belgian Anti-Money Laundering Act defines **"high-risk third countries"** as countries that have, among other things, been identified as high-risk by the **Financial Action Task Force (FATF)**.
With regard to high-risk third countries, **Enhanced Due Diligence (EDD) measures must always be applied**, including:

- Obtaining additional information on the customer and the ultimate beneficial owner(s) (UBOs);
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds and the source of wealth of the customer and the ultimate beneficial owner(s);
- Obtaining information on the reasons for the intended or completed transactions;
- Obtaining approval from senior management before establishing or continuing the business relationship;
- Conducting enhanced monitoring of the business relationship by increasing the number and frequency of reviews and by identifying transaction patterns that require further scrutiny;
- Where appropriate, ensuring that the first payment is made through an account in the customer's name held with a credit institution that applies customer due diligence standards at least equivalent to those laid down in this Act.

The grey list
Countries on this list are considered to be under **increased monitoring** by the FATF. The FATF does not recommend countermeasures against countries on the grey list, nor does it prohibit business with them. Instead, these countries are required to improve their AML/CFT control frameworks and report on their progress to the FATF.

The Belgian Anti-Money Laundering Act does **not distinguish between the FATF black list and grey list**. Rather, it refers to countries presenting a **high geographical risk**. Based on the FATF's classifications, this primarily concerns the countries on the black list.

Nevertheless, it is advisable to apply **Enhanced Due Diligence (EDD)** when dealing with counterparties or transactions linked to countries on the grey list.

Attention

Business with these countries is prohibited OR is subject of the strictest EDD controls.

You can consult official lists published by the European Commission and the Financial Action Task Force. These lists are regularly updated and must be checked each time.

Attention

If the risks cannot be sufficiently mitigated, you must refuse the transaction or relationship.

Always document your assessment, the measures taken, and your decision. This information must be available upon request, for example during an AML inspection.

Practical example

A supplier approaches you offering a parcel of rough diamonds. His company is registered in a country currently on the FATF grey list.

Step 1 — Flag the geography: The country of origin alone places this in a higher-risk category. You cannot apply standard due diligence.
Step 2 — Enhanced KYC: Ask for full UBO details, verified identity documents, and detailed information on how the company operates.
Step 3 — Source of funds: Request evidence of how the supplier acquired these diamonds and where the payment funds originate.
Step 4 — Bank check: Verify that the bank the supplier uses is reputable and operates with adequate AML controls.
Step 5 — Management approval: Escalate for sign-off before committing to the relationship.
Step 6 — Ongoing: If you proceed, review the relationship more frequently than for a standard counterparty.

4.6.4 Engaging with a counterparty or transaction linked to a sanctioned country or jurisdiction

What are sanctions?

Sanctions are legal restrictions imposed by governments or international bodies that restrict op prohibit business with certain countries, entities or individuals. Unlike the FATF grey list (which requires EDD), sanctions can outright prohibit a transaction.

The FPS Finance is responsible for monitoring and ensuring compliance with the international financial sanctions imposed by the EU.

A key example are the EU sanctions against Russia, because of Russia's war against Ukraine:

Since 1 January 2024, Russian diamonds fall under EU sanctions which makes it legally prohibited to import or export diamonds of Russian origin. This measure applies to:

- All non-industrial natural diamonds (rough and polished) equal to or larger than 0,5 carat;
- All non-industrial synthetic diamonds equal to or larger than 0,5 carat;
- The ban applies regardless of where the diamonds are shipped from. Routing goods via a third country (such as Dubai) does NOT make an otherwise prohibited transaction legal.

Attention

If you want to import or export diamonds suspected of being of Russian origin and you cannot provide the proper documentation to prove otherwise, these diamonds will be considered prohibited goods, and customs will open an investigation.

Industrial diamonds are not covered by these sanctions.

The different stages of the EU Sanctions against Russia, are:

- The first stage: started on January 1, 2024: This was the moment when the import of diamonds of Russian origin or diamonds coming directly from Russia became illegal (= direct ban).
- The second stage: started on March 1, 2024: As of this moment, the indirect import of Russian diamonds (for example, when they were first polished in a third country like India) has also become illegal. During this stage, which is also known as the 'Sunrise Period', documentary evidence is required to prove the origin of diamonds (and that they are non-Russian) when importing diamonds into Belgium via the Diamond Office. All diamonds in scope during this period (March 1 until September 1, 2024) are natural, non-industrial, rough and polished diamonds equal to or larger than 1 carat.
- The third stage: in effect since September 1, 2024: From this moment, diamonds in scope are expanded with synthetic diamonds, so diamonds in scope are natural and synthetic, non-industrial, rough, and polished diamonds equal to or larger than 0.5 carat. Also, from this moment, Belgian Registered Diamond Companies will be able to regularize their existing stock of goods, consisting of diamonds of Russian or unknown origin. This is the so-called 'Grandfathering Principle'.
- The fourth stage: started on March 1, 2025: There is a new requirement added for mixed origin rough import in the Sixteenth Sanction Package against Russia. When you're importing rough diamonds into the EU, that are in scope (all natural, non-industrial, rough diamonds equal to or larger than 0.5 carat), KP Certificates must now mention all countries of origin. Mixed origin*** is no longer accepted on the KP Certificate.
- Fifth stage: completed by January 1, 2026: From 1 January 2026, traders who import polished diamonds that fall within the scope* must add a Due Diligence Statement on Diamond Origin to their customs declaration. *natural polished goods equal to or larger than 0.5 carats

It is also important to note that the Russian diamond producer Alrosa is included on the European sanctions list. Consequently, you may not purchase diamonds from Alrosa, even if the diamonds concerned are smaller than 0.5 carats.

For detailed guidance on the EU sanctions against Russia and what documentation is required when importing and exporting diamonds, see:

Practical example

A client offers to sell you polished diamonds (each above 0.5 ct) that were shipped from Dubai. The accompanying documents are vague about the original country of mining.

Step 1 — Flag the ambiguity: Dubai is a major transit hub. Shipping from Dubai does not prove the diamonds are not of Russian origin.
Step 2 — Request documentation: Ask for the full chain of custody — mining country, Kimberley Process certificate, and all import/export documents from the country of origin.
Step 3 — Assess: If the client cannot or will not provide documentation proving non-Russian origin, you must treat the goods as potentially prohibited.
Step 4 — Decision: Refuse the transaction.

If you suspect that someone is intentionally trying to bypass sanctions, you must report this to the CFI.

4.6.5 Transactions with a US Nexus

A transaction may have a US nexus when it involves a connection to the United States, such as a US person, a US company, a payment in US dollars (USD), a US financial institution, or goods destined for the US market. Even when a diamond trader is not established in the United States, US regulations and sanctions may still become relevant if such a connection exists.

Transactions with a US nexus should be treated as higher risk and require Enhanced Due Diligence (EDD). This includes verifying the identity of all parties involved, screening counterparties against applicable sanctions lists, understanding the origin and destination of funds, and ensuring that the transaction does not involve prohibited persons, entities, or goods. Particular attention should be paid to USD payments, as these are often processed through the US financial system and may therefore be subject to additional scrutiny.

👉 Always document the US nexus identified, the checks performed, and the rationale for proceeding with or refusing the transaction.

4.6.6 Having a counterparty who wants to pay through a third party

A third-party payment occurs when a person or company other than the invoiced counterparty makes the payment. As a general rule: the party who is invoiced should also be the party who pays.

Third-party payments are considered a **high-risk situation** because they can be used to hide the true origin of funds or the identity of the parties involved.

You may only accept a third-party payment if:

- **The transaction is fully transparent** : You clearly understand who is paying, on whose behalf, and for what reason
- **There is a written agreement between all parties involved**: This agreement must explain the relationship and justify the payment structure
- **You have given your explicit consent**: You must assess the situation and agree to the arrangement before the payment is made

In practice, many banks consider third-party payments to be high risk and may refuse to process them.

Attention
If you suspect that a third-party payment is linked to illegal activity, you must **refuse the transaction**.

Always document the reason why you accept or refuse a third-party payment. For guidance, you can refer to the AWDC Best Practice Guide, which includes a template for a three-party agreement.

Practical Example

You invoice a diamond buyer in Hong Kong for a parcel of polished diamonds. Shortly before the payment is due, you receive a message that the payment will come from a company in a different country — a company you have never heard of and which is not mentioned anywhere in your KYC file.

Step 1 — Stop: Do not accept the payment until you understand who is paying and why.
Step 2 — Request a written explanation: Ask for a written agreement signed by all three parties explaining the relationship and the reason for the third-party payment.
Step 3 — Verify the third party: Apply KYC and a risk assessment to the third party — they are now part of your transaction.
Step 4 — Assess: If the explanation is satisfactory and the third party is verifiable, you may proceed — with documented consent.
Step 5 — Red flag: If the buyer cannot or will not explain the arrangement, refuse the payment and consider whether a CFI report is required.

4.6.7 Having a counterparty who wants to pay cash

Why are cash payments a high-risk situation?

They are inherently difficult to trace. Unlike bank transfers, cash leaves little or no audit trail, which makes it more attractive for criminals who want to hide the origin of funds.

For this reason, cash paymens – especially large ones – are treated as a high-risk indicator that requires Enhanced Due Diligence.

Cash payment limits you must know

Scope	Limit	What this means
Belgium	€3,000 per transaction	This is a strict legal maximum. Splitting payments into smaller amounts to stay below this limit (known as 'structuring') is also prohibited.
EU border (entering/leaving)	€10,000 declaration threshold	Anyone crossing an EU border with €10,000 or more in cash must declare it to customs.
Outside Belgium	Local rules apply	You must always comply with the cash payment rules of the country where the transaction takes place.

Attention

If a counterparty insists on paying an amount of over 3.000 euros in cash, without a clear or legitimate reason, or if the payment structure appears unusual, you should refuse the transaction, consider ending the business relationship and report to the CFI.

Always document the reason for accepting or refusing cash payments, and ensure that all legal limits are strictly respected. This information must be available upon request, for example during an AML inspection.

What must you do when a counterparty insists on a cash payment?

- Assess whether the requested cash amount is within the legal limit (Belgium: €3,000).
- If it exceeds the limit: refuse immediately.
- If it is within the limit but seems unusual or unjustified for the transaction: apply EDD — ask for an explanation and verify the source of funds.
- Document your decision — whether you accepted or refused — and the reasons for it.
- If you cannot get a satisfactory explanation, refuse and consider whether a CFI report is required.

Practical Example

During an ongoing business relationship, a client you have dealt with for two years informs you that he wants to pay €10,000 in cash for his latest purchase. You have always received bank transfers from him before.

Step 1 — Legal check: €10,000 in cash in Belgium exceeds the €3,000 legal limit. This is not a judgement call — it is prohibited by law.
Step 2 — Refuse: You must decline the cash payment regardless of your existing relationship or previous risk classification.
Step 3 — Reassess the relationship: The request itself is a red flag and must trigger a reassessment of the client's risk profile. A previously 'low-risk' client does not stay low-risk when they ask for something illegal.
Step 4 — Document: Record the request, your refusal, and the grounds for it.
Step 5 — Report if needed: If the request suggests suspicious intent, report to the CFI.

Do the Risk Assessment-Check:

Be sure to be able to answer clearly:

- Who is the counterparty? (KYC)
- Who owns the counterparty? (UBO's identified and verified)
- Why are you doing business? (purpose and nature of the business relationship)
- Are there any red flags? (PEP, Sanctions, high-risk country, third party payment, cash payment)
- **Can the risk(s) be mitigated?** – Through EDD measures and or internal approval by the senior management
- **Do the transactions make sense?** – Are they consistent with the **counterparty's** profile and business activity?
- **What is your decision?** Accept, accept with conditions, or refuse. Document this in writing!

Test Your Knowledge

(correct answers are provided at the end of this syllabus)

1. During a business relationship, a client wants to pay you €10,000 in cash in Belgium. What do you do?
   a. Refuse, end the relationship if appropriate, and report to the CFI — cash payments of this size are prohibited in Belgium
   b. Accept — no cash limit exists in Belgium, but treat the client as high risk
   c. Accept if the amount is below €20,000 and update your risk assessment
   d. The client was previously assessed as low risk, so nothing changes

2. Which person can be considered a PEP (Politically Exposed Person)?
   a. People who have been criminally charged — medium to high risk; increased vigilance required
   b. People who hold or have held a prominent public position — medium to high risk; increased vigilance required
   c. People who hold or have held a prominent public position — it is prohibited to do business with them
   d. People who have been criminally charged — it is prohibited to do business with them

3. A diamond trader finds an unusual transaction — for example, an unusually large purchase. What must the trader do?Treat the counterparty as low risk
   a. Ignore it unless there is direct proof of money laundering
   b. Discuss internally but take no further action and make no written record
   c. Ask the client for an explanation but do not investigate further — privacy law prevents it
   d. Investigate and prepare a written analysis. If money laundering is suspected, report to the CFI

4. A client proposes to use a third party to make payment. How do you respond?
   a. Accept via a recognised intermediary without requiring documentation
   b. Refuse the payment and ask the client for the reason and source of funds; verify before proceeding
   c. Refuse and inform the client that only direct bank transfers are permitted; report immediately to the CFI
   d. Accept as long as the amount is below the €3,000 cash threshold

5. If a high-risk client shows no suspicious activity, their file only needs to be updated when an unusual event occurs.
    a. True
    b. False

6. There are currently 3 countries on the FATF black list: North Korea and Iran. What is the third?

7. Which diamond type is NOT covered by EU sanctions on Russian diamonds?
    a. Polished diamonds over 0.5 carat
    b. Synthetic (lab-grown) diamonds over 0.5 carat
    c. Industrial diamonds over 0.5 carat
    d. Rough diamonds over 0.5 carat

8. Diamonds suspected of Russian origin are missing the correct documentation. What happens?
    a. Placed in quarantine and tested
    b. Returned to the exporting country
    c. Treated as prohibited goods — customs opens an investigation
    d. Temporarily admitted pending clarification

9. A Belgian trader buys Russian rough non-industrial diamonds (>0.5 ct) from a dealer in Dubai in 2024. This is permitted because the goods come from the UAE.
    a. True
    b. False

10. On what date did the EU ban on Russian non-industrial diamond imports begin?

11. Which Belgian government service is responsible for monitoring the financial sanctions imposed by the EU?
    a. FPS Finance
    b. CFI
    c. FPS Economy

Chapter Five: Reporting Suspicious Activity

What can I find in this chapter?

5.1 What is reporting suspicious activity and why is it important?

5.2 When do you have to report suspicious activity?

5.3 Protection of the reporting person by the government

5.4 Where and how to report suspicious activity

5.1 What is reporting suspicious activity and why is it important?

If a transaction or business relationship seems unusual, inconsistent, or suspicious — even if you have no proof of wrongdoing — you must stop and report it to the CFI (Financial Intelligence Processing Unit), without delay.

This is called reporting suspicious activity, and it is a legal obligation.

Attention
The decision not to proceed with a transaction and to notify the CFI must be clearly documented in writing. You must also **be able to present an overview of all reports** submitted to the CFI during an AML inspection. Note that, where applicable, **it works in your favor to demonstrate that you have made such notifications.**

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

5.2 When must you report suspicious activity?

You decide whether to report to the Financial Intelligence Processing Unit (CFI) based on the risk assessment you did for this specific client, supplier or transaction, using the risk scorecards (see annex A, B and C).

You must report to the CFI if:

- Your risk assessment identifies at least one unacceptable (red) risk (see Annex A, B, or C), or
- Multiple risk factors make it unsafe to proceed

In such cases, the counterparty must be refused or the existing relationship terminated **and the Financial Intelligence Processing Unit (CFI) must be informed**:

- **before the transaction** is carried out and you must indicate the expected timing of the transaction.
- **immediately after** (if reporting beforehand was not possible) and clearly **explain why prior notification was not possible**.

Attention
It is **prohibited to inform** your counterparty or other third parties about the fact that you notified the CFI.

You must report whenever a situation appears **unusual, inconsistent, or suspicious**, even if you do not have proof of wrongdoing.

Examples:

- **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:** A 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 are used:** Such as third-party payments without a clear justification.
- **The counterparty is linked to criminal activity, sanctions, or negative media:** This includes fraud, corruption, tax evasion, or other illegal activities.
- **You suspect the use of false or forged documents**
- **The transaction involves high-risk countries without a clear explanation**
- **The counterparty insists on secrecy or unusual confidentiality**

Attention
You must also report attempted transactions, even if they were not completed.

5.3 Protection of the reporting person by the government

The diamond trader (or any employee) who submits a report is **protected by the authorities** against threats or acts of aggression, when he is good faith.

The Financial Intelligence Processing Unit treats all reports confidentially and does not share them with third parties.

Anyone who provides information or reports in good faith cannot be punished or held liable in any way (civil, criminal, or disciplinary) and **is therefore legally protected** (this is called 'legal immunity').

5.4 Where and how to report suspicious activity?

In Belgium, suspicious activities must be reported to the **Cel voor Financiële Informatieverwerking (CFI) / Cellule de Traitement des Informations Financières (CTIF)**.

Reports to the Financial Intelligence Processing Unit (CFI) must be submitted via the **goAML application**.

To do so, you first need to **register and create an account by sending a request** to goaml.helpdesk@ctif-cfi.be.

It is the AML officer's responsibility to create an account on goAML and report suspicious transactions to the CFI.

Your notification report should include:

- Who the counterparty is (identification details)
- What the transaction was
- Why it seemed suspicious
- Any supporting documents

Key Principles to Respect

- **Do not wait until you are100% sure:** suspicion is enough to report, you don't need proof of wrongdoing.
- **Don't tell the counterparty (no 'tipping-off'):** you are strictly prohibited from informing the **counterparty** that a report has been made.
- **Act without delay:** reports must be made as soon as the suspicion arises and before the transaction takes place.
- **Your are protected** and cannot be punished or held liable in any way (reporting in good faith gives you legal immunity)

Practical Example 1

A client wants to purchase a polished diamond for €8,500. He proposes the following:

- €2,900 in cash today
- €2,900 in cash tomorrow
- The remaining amount later, again in cash

Even if you inform him that the legally accepted threshold for cash payments in Belgium is 3000 euros, he insists on splitting the payments and explicitly mentions he wants to "stay below the limit."

→ This is a clear example of structuring: deliberately breaking down a transaction into smaller amounts to avoid legal limits or controls (in this case, the €3,000 cash payment limit in Belgium).

Why report to the CFI?

- Clear attempt to circumvent the legal cash limit
- The payment structure is artificial and has no economic justification
- Indicates a potential attempt to hide the origin of funds or avoid traceability

Even though each individual payment is below €3,000, the intent to bypass the law is explicit, which creates a strong suspicion.

Practical Example 2

A new supplier based in South Africa (which has been on the FATF grey list since 2023 due to weaknesses in combating money laundering and ensuring transparency) offers a parcel of rough diamonds at an attractive price.

During the onboarding:

- The supplier provides incomplete KYC information
- There is no clear documentation on the origin of the diamonds
- When asked for additional details, the supplier becomes evasive and pushes to proceed quickly

→ Why is this high risk? Countries on the FATF grey list are identified as having strategic deficiencies in their AML/CFT framework, which increases the risk of money laundering or illicit trade.

Why report to the CFI?

- Counterparty located in a higher-risk jurisdiction (FATF grey list)
- Lack of transparency regarding both the supplier (incomplete KYC file) and the goods (no documentary evidence, proving the origin)
- Pressure to proceed despite missing or unclear information

→ The combination of geographical risk + incomplete KYC + evasive behaviour creates a reasonable suspicion of money laundering or illicit origin of goods, triggering a reporting obligation.

Test Your Knowledge

(correct answers are provided at the end of this syllabus)

1. Am I legally required to report suspicious transactions to the CFI?
    a. Yes. I am required to do so and have immunity — no risk of prosecution
    b. No. Reporting is voluntary
    c. Yes, but only for transactions above a certain amount or from certain countries
    d. Yes, but only if I am certain that money laundering has taken place

Chapter Six: How to Prepare for an AML Inspection

What can I find in this chapter?

6.1 What is an AML inspection

6.2 How does an AML inspection proceed?

6.3 What information must you be able to show?

6.4 Practical tips and tricks on 'how to survive' an AML inspection

6.1 What is an AML inspection?

An AML inspection is an official visit by an inspector from the Federale Overheidsdienst Economie.

During the inspection, the inspector verifies whether your company complies with AML legislation in its day-to-day operations, including the correct application of KYC, risk assessments, internal procedures, and the reporting of suspicious activities.

An inspection is not something to fear if you are well prepared. If your files are complete, your processes are clear, and you understand AML law, an inspection simply confirms that your business is running as it should.

An AML inspection is not a one-time snapshot, but a direct reflection of how your business operates every day.

6.2 How does an AML inspection proceed?

During an inspection, the inspector will typically:

- Select around 20 to 30 client or supplier files (going back up to 3 years)
- Check whether your AML files are complete and well-organised
- Check whether you have carried out proper risk assessments
- Check whether you correctly identify high-risk counterparties
- Ask you to explain your decisions (for example, why you accepted a counterparty)
- Check whether your KYC information is up to date
- Check compliance with cash payment limits and suspicious transaction reporting

The inspection can last several hours — sometimes a full working day. The better organized your files are, the faster it goes.

Attention

The AML officer(s) are responsible for handling the inspection, responding to questions, and providing the requested documents. However, if the AML officer(s) are not present, another employee should be able to take over this role and provide the inspectors with information.

6.3 What information must you be able to show?

During the inspection, the inspector will ask you to show different documents. Make sure you have them all **easily and physically accessible** so that the inspection can proceed efficiently.

This is a checklist of all documents that must be **readily available upon request** of the inspector:

- The names of the **ultimate responsible AML officer** (senior management level) and the **'operational' AML officer** who is is responsible for the practical implementation of AML procedures on a day-to-day basis.
- **An internal AML policy**, updated and signed annually (you can use the AML Policy Template developed by the Antwerp World Diamond Centre; (See chapter 7 – AML Templates, Tools and Manuals offered by AWDC).
- **Your AML certificate**, as proof that you have either attended the AML webinar annually or passed the AML exam.
- **A complete AML file for each counterparty**, including KYC information, a risk assessment, and a documented conclusion on how to proceed with the business relation (accept, accept with conditions, or refuse). (You may use the KYC and Risk Assessment Conclusion Template developed by the Antwerp World Diamond Centre; (See chapter 7 – AML Templates, Tools and Manuals offered by AWDC).
- **Historical AML files for each counterparty.**
- A physical or digital **copy of your AML Activity Report.**
- **Invoices** covering a period of up to three years.
- **Cashbooks**. If these are not physically available in your office, the inspector may request them directly from your accountant or bookkeeper.

Attention

In addition to reviewing your documentation, **inspectors will test your knowledge of AML legislation** by asking practical questions. These may include what qualifies as a suspicious transaction, how you would handle such a situation, what a UBO (Ultimate Beneficial Owner) is, and what the role of the CFI is. It is therefore essential not only to have your documents in order, but also to **clearly understand the AML obligations and how they apply in practice.**

6.4 Practical tips and tricks on how to get through an AML inspection

Make sure you are well prepared for an AML inspection **at all times**. Inspectors may visit at any moment, often without prior notice.

The following tips will help you handle an inspection smoothly and keep its duration as short as possible:

- Ensure that **you are available for inspectors** from the Federale Overheidsdienst Economie and present at your company's registered address. If you are repeatedly absent or refuse an inspection, a police report may be drawn up.
- **Keep all required information well organized and easily accessible.** This prevents you from having to search for documents during the inspection, which can create unnecessary stress and prolong the process. **Working with a digital tool such as KYCP can help you structure, store, and keep your documents up to date** (See chapter 7 – AML Templates, Tools and Manuals offered by AWDC).
- **Always be honest and transparent.** Do not try to hide or downplay mistakes, and do not hesitate to admit when something is not perfect.
- **Make sure you understand AML legislation**. Inspectors may ask theoretical questions that you should be able to answer, such as what a UBO is or what the role of the Financial Intelligence Processing Unit is.
- Show that you have reported to the CFI when needed. It is important to note that **it works in your favor if you can demonstrate that you have made such reports when necessary**.
- Show ongoing monitoring. Demonstrate that you regularly review your business relationships and keep AML information up to date.
- Train your staff. Make sure employees know your internal AML procedures and are regularly updated.

Attention
During an inspection, it is the responsibility of one of the AML officers to answer the inspector's questions and provide the requested documents. **However, if neither of them is present, another employee must be able to take over this role.**

Test Your Knowledge

(correct answers are provided at the end of this syllabus)

1. An AML inspection is announced in advance so that you have time to prepare your files.
    a. True
    b. False

2. During an AML inspection, the inspector selects a number of counterparty files to review. How many files are typically selected, and how far back can they go?
    a. 5 to 10 files, going back up to 1 year
    b. 20 to 30 files, going back up to 3 years
    c. 50 to 100 files, going back up to 5 years
    d. All files from the past year

3. The AML officer is not available on the day of an inspection. What happens?
    a. The inspection is automatically postponed until the AML officer is present
    b. The inspection cannot proceed — only the AML officer is legally authorised to respond
    c. Another employee must be able to take over and provide the inspector with the requested information
    d. The company can submit the documents by email within 5 working days

4. Which of the following is NOT something an inspector may ask during an AML inspection?
    a. To explain why you accepted a specific counterparty
    b. To show your AML certificate
    c. To demonstrate that you have reported suspicious transactions to the CFI when required
    d. To provide a list of all transactions above €1,000 for the past 10 years

Chapter Seven: AML Templates, Tools and Manuals Offered by AWDC

What can I find in this chapter?

7.1 Ready-to-use AML templates

7.2 Tools

7.3 Manuals

7.1 Ready-to-use AML templates

AWDC provides three ready-to-use templates. All are approved by or developed in line with FPS Economy requirements.

AML Policy template:

This Anti-Money Laundering (AML) Policy Template is designed as a practical guideline to help Belgian-registered diamond companies establish their internal AML policy. It has been approved by the Federale Overheidsdienst Economie and must be tailored to the specific situation of each company.

AML Client Letters:

AML Client Letters are standard letters to send to your clients or suppliers when you need KYC information from them. Ask them to complete the missing information and send the file back to you.

KYC and Risk Assessment Conclusion Template:

You can use this template to clearly justify and document your decision on whether to accept, accept with conditions, or refuse a counterparty.

7.2 Tools

7.2.1 KYCP: a key AML tool for diamond traders

To help diamond traders comply with AML legislation, AWDC provides several practical tools. The most important one is **KYCP (Know Your Customer Platform)**.

KYCP is an online platform that helps you **collect, manage, and update all AML-related information** about your counterparties in one central place. It supports you throughout the entire due diligence process:

- Identify and verify your counterparties
- Assess their risk profile
- Keep AML documents and information up to date
- Document and justify your decisions (accept, reject, or end a relationship)

Integrated screening tools: GRID and ORBIS

When using KYCP, you also get access to powerful databases and screening tools, which are fully integrated in the KYCP module:

- **ORBIS**: a global company database that provides **detailed information on companies,** including:
- Ownership structures (including UBOs)
- Financial data
- Corporate links

This helps you better understand who you are doing business with.

- **GRID**: A comprehensive database used to screen and monitor counterparties for **risks related to financial crime**. It includes data on:
- Politically Exposed Persons (PEPs)
- Sanctions lists
- Negative media

Together, these tools support a complete, consistent, and well-documented risk assessment process. They help you decide whether to onboard a counterparty or not.

If you already have a KYCP-account, login here:

If you are not registered for KYCP yet, then request your free account via helpdesk@awdc.be

For more information on KYCP, visit our website via the QR code below.
New to KYCP? Watch our short video via the QR below — it walks you through registration step by step and shows you what KYCP can do for you.

7.2.2 Ultimate Beneficial Owners (UBO) Register

The Belgian UBO Register lists the real owners(Ultimate Beneficial Owners), fully or partially, of all Belgian companies, non-profit organizations, foundations, and trusts.

Use this register to verify who really owns or controls a Belgian company you want to do business with.

7.2.3 Tools to help you when doing business with sanctioned countries

If you want to assess whether it is safe to do business with a counterparty based in a country subject to sanctions or embargoes, or in a country that is not a member of the Kimberley Process, it is strongly recommended to use these tools to evaluate the risks associated with the business relationship and to determine whether it is still possible to proceed, provided that appropriate risk-mitigating measures are taken.

FATF Black and Grey List:

Shows which countries have weaknesses in fighting money laundering and terrorist financing. Countries on the Black List are the highest risk countries (Myanmar, Iran, and North Korea), those on the Grey List are under increased monitoring.

Kimberley Process Participants List:

Shows which countries are part of the Kimberley Process — the international certification scheme to keep conflict diamonds out of the market. If a country is not on this list, extra caution is required.

7.2.4 CFI Platform to notify suspicious transactions or facts

As a diamond trader, you must always notify the CFI when you encounter a suspicious transaction or fact that could possibly relate to money laundering or financing of terrorism.

Reports to the Financial Intelligence Processing Unit (CFI) must be submitted via the **goAML application.**

To do so, you first need to **register and create an account by sending a request to goaml.helpdesk@ctif-cfi.be.**

It is the AML officer's responsibility to create an account on goAML and report suspicious transactions to the CFI.

7.3 Manuals

Submit your AML Report

Manual:

Manual: Access to Diamond Supervision (needed for submitting your AML report):

KYCP:

New to KYCP? Watch our short video. It walks you through registration and shows you what KYCP can do for you.

You can find the video at the bottom of this page:

Glossary

A

AML-certificate
Proof of successful completion of AML training.

AML-inspection
Audit by FPS Economy checking compliance with AML obligations.

AML obligations (8 steps)
The core compliance duties for diamond traders, including training, KYC, risk assessment.

AML-officer
The person responsible for AML compliance within the company (typically a director), ensuring procedures are followed and risks are monitored.

AML-policy
Internal document outlining how your company complies with AML rules.

AML-report (annual)
A yearly report submitted via the government platform summarizing AML activities.

AML-reporting procedure
Internal process explaining how and when suspicious activities are reported.

AML-seminar
Mandatory yearly training on AML compliance.

Anti-Money Laundering (AML) law
Legal framework requiring companies to prevent, detect, and report money laundering by applying KYC, risk assessment, and reporting obligations.

B

Bankruptcy
A legal process where a person or company that cannot pay its debts is declared insolvent and its assets are used to repay creditors.

Best Practice Seminar
Optional training focused on transparency and good practices.

C

Cel voor Financiële Informatieverwerking (CFI)
Belgian Financial Intelligence Unit receiving and analyzing suspicious activity reports.

Client
A person or company you sell to.

Complex Ownership Structure
A company setup with multiple layers of owners or entities, making it hard to see who really controls it.

E

Enhanced due diligence (EDD)
Additional checks required for high-risk clients (e.g. PEPs, high-risk countries).

G

General Data Protection Regulation (GDPR)
(General Data Protection Regulation): An EU law that protects people's personal data and privacy.

H

High-risk client
A client requiring extra scrutiny (e.g. PEPs, high-risk countries, unusual transactions).

High-risk country
A country identified as having increased risk of money laundering or weak AML controls.

I

Itsme
A secure app used in Belgium to verify your identity and log into official services.

K

KYC (Know Your Customer / Counterparty)
The process of identifying and verifying clients and suppliers, understanding their activities, and assessing risk.

KYC file
A documented file proving you:
• Know your counterparty
• Understand the relationship
• Assessed the risk
• Justified your decision

KYCP (Know Your Counterparty Platform)
Digital tool for managing KYC, screening risks, and monitoring clients.

M

Moody's
A financial platform that provides credit ratings and risk analysis for companies and governments.

Money laundering
The process of hiding the illegal origin of money to make it appear legitimate.

MyMinFin
An online Belgian government platform where you manage your taxes and financial information.

N

Natural Person
The business is operated by an individual without a separate legal entity like a corporation.

Non-compliance
Failure to meet AML requirements → may result in fines or sanctions.

O

Ongoing monitoring
Continuous review of clients/suppliers during the business relationship to ensure risk remains acceptable.

P

Politically Exposed Person (PEP)
A person with a prominent public function (e.g. minister), including their family and close associates, considered higher risk.

R

Record keeping
Obligation to keep AML/KYC data for 10 years after the relationship ends.

Red flags
Warning signs of potential money laundering, such as:
• Unusual payment methods
• Lack of transparency
• High cash usage
• Complex ownership structures

Registered Diamond Companies (.be)
Government platform for AML reporting, training, and company registration.

Risk assessment
The process of evaluating whether a client or supplier poses a risk before doing business.

Role Management Administration (RMA)
A system used to assign, manage, and control user roles and permissions within government platforms (e.g. MyMinFin), ensuring that only authorized individuals can access and perform specific administrative or compliance-related tasks on behalf of a company.

S

Sanctions
Restrictions imposed by governments or international bodies prohibiting business with certain individuals, entities, or countries.

Sanctions hit
A match between your counterparty and a sanctions list → business must stop immediately.

Difference with PEP:
• PEP = allowed with caution
• Sanctioned person = prohibited

Sanctions lists
Official lists (EU, UN, OFAC) of sanctioned persons/entities.

Sanctions screening
The process of checking whether a client, supplier, or UBO appears on a sanctions list.

Supplier
A person or company you buy from.

Supply Chain Due Diligence (SCDD)
Process of ensuring diamonds are ethically sourced (human rights, conflict-free, etc.).

SCDD vs AML
• AML → financial crime
• SCDD → ethical sourcing

Suspicious transaction report (STR)
A mandatory report submitted when you suspect money laundering or criminal activity.

T

Third-party payment
Payment made by someone other than the invoiced client; considered high-risk and requires justification.

U

Ultimate Beneficial Owner (UBO)
The real individual(s) who ultimately own or control a company (≥25% ownership or control).

Answer Key

Chapter One

1. What is the maximum amount of the fine for a legal entity under Belgian anti-money laundering legislation in case of non-compliance by a diamond trader
    a. 1.000.000 euro
    b. 2.000.000 euro
    c. 3.000.000 euro
    d. 1.250.000 euro

- Which Belgian government service is responsible for conducting AML inspections?
    - FPS Finance
    - CFI
    - FPS Economy

Chapter Two

1. What is the deadline for submitting the annual AML report?
    a. 1 April
    b. 31 March
    c. 31 May
    d. 1 June

2. How often must you attend an AML training if you have not passed the AML exam?
    a. Every year
    b. Every two years
    c. Every three years
    d. Every four years

3. An AML officer can independently decide to use company resources to meet AML obligations.
    a. True
    b. False

4. Only the AML officer (or the person appointed by management) can prepare the annual AML report.
    a. True
    b. False

5. Which Belgian government body monitors EU financial sanctions? FPS Finance

6. How many times per year must you attend an AML training if you have not passed the exam? (Enter a number) 1

Chapter Three

1. A client refuses to provide an identity document or disclose the names of the UBOs. What do you do?
   a. Continue the relationship, document the refusal, and adjust your risk assessment
   b. Respect the client's privacy and continue the relationship
   c. Refuse the relationship or transaction. If money laundering is suspected, report to the CFI
   d. Continue the relationship but report to the federal judicial police

2. After a business relationship ends, how long must records be kept? 10 years. After this period, documents must be deleted or destroyed.

3. Your search finds no information about a counterparty. What do you do?
   a. Treat the counterparty as low risk
   b. Treat as neutral risk and document the search attempt
   c. Do not proceed — you cannot meet your identification obligation
   d. Continue without further verification

4. What steps must a diamond trader follow to identify UBOs of a foreign company?
   a. Ask the company or representative to sign a declaration
   b. Take reasonable steps to collect and verify information (name, address, directors, UBOs) and keep the documents
   c. Only collect director information if the risk is high
   d. Collect only name and address — asking for more violates GDPR

5. KYC data should be updated every year for high-risk clients, and every 2 to 3 years for other clients.
   a. True
   b. False

6. What minimum ownership percentage qualifies someone as a UBO in Belgium? 25%

Chapter Four

1. During a business relationship, a client wants to pay you €10,000 in cash in Belgium. What do you do?
   a. Refuse, end the relationship if appropriate, and report to the CFI — cash payments of this size are prohibited in Belgium
   b. Accept — no cash limit exists in Belgium, but treat the client as high risk
   c. Accept if the amount is below €20,000 and update your risk assessment
   d. The client was previously assessed as low risk, so nothing changes

2. Which person can be considered a PEP (Politically Exposed Person)?
   a. People who have been criminally charged — medium to high risk; increased vigilance required
   b. People who hold or have held a prominent public position — medium to high risk; increased vigilance required
   c. People who hold or have held a prominent public position — it is prohibited to do business with them
   d. People who have been criminally charged — it is prohibited to do business with them

3. A diamond trader finds an unusual transaction — for example, an unusually large purchase. What must the trader do?Treat the counterparty as low risk
   a. Ignore it unless there is direct proof of money laundering
   b. Discuss internally but take no further action and make no written record
   c. Ask the client for an explanation but do not investigate further — privacy law prevents it
   d. Investigate and prepare a written analysis. If money laundering is suspected, report to the CFI

4. A client proposes to use a third party to make payment. How do you respond?
   a. Accept via a recognised intermediary without requiring documentation
   b. Refuse the payment and ask the client for the reason and source of funds; verify before proceeding
   c. Refuse and inform the client that only direct bank transfers are permitted; report immediately to the CFI
   d. Accept as long as the amount is below the €3,000 cash threshold

5. If a high-risk client shows no suspicious activity, their file only needs to be updated when an unusual event occurs.
    a. True
    b. False - high-risk counterparties must be reviewed at least every 12 months, regardless of whether an unusual event has occurred

6. There are currently 3 countries on the FATF black list: North Korea and Iran. What is the third? Myanmar (Burma)

7. Which diamond type is NOT covered by EU sanctions on Russian diamonds?
    a. Polished diamonds over 0.5 carat
    b. Synthetic (lab-grown) diamonds over 0.5 carat
    c. Industrial diamonds over 0.5 carat
    d. Rough diamonds over 0.5 carat

8. Diamonds suspected of Russian origin are missing the correct documentation. What happens?
    a. Placed in quarantine and tested
    b. Returned to the exporting country
    c. Treated as prohibited goods — customs opens an investigation
    d. Temporarily admitted pending clarification

9. A Belgian trader buys Russian rough non-industrial diamonds (>0.5 ct) from a dealer in Dubai in 2024. This is permitted because the goods come from the UAE.
    a. True
    b. False - the origin of the diamonds, not the shipping location, determines whether the transaction is prohibited under EU sanctions

10. On what date did the EU ban on Russian non-industrial diamond imports begin? 1 January, 2024

11. Which Belgian government service is responsible for monitoring the financial sanctions imposed by the EU?
    a. FPS Finance
    b. CFI
    c. FPS Economy

Chapter Five

1. Am I legally required to report suspicious transactions to the CFI?
    a. Yes. I am required to do so and have immunity — no risk of prosecution
    b. No. Reporting is voluntary
    c. Yes, but only for transactions above a certain amount or from certain countries
    d. Yes, but only if I am certain that money laundering has taken place

Chapter Six

1. An AML inspection is announced in advance so that you have time to prepare your files.
    a. True
    b. False - inspectors can visit at any time, often without prior notice. Your files must be ready at all times.

2. During an AML inspection, the inspector selects a number of counterparty files to review. How many files are typically selected, and how far back can they go?
    a. 5 to 10 files, going back up to 1 year
    b. 20 to 30 files, going back up to 3 years
    c. 50 to 100 files, going back up to 5 years
    d. All files from the past year

3. The AML officer is not available on the day of an inspection. What happens?
    a. The inspection is automatically postponed until the AML officer is present
    b. The inspection cannot proceed — only the AML officer is legally authorised to respond
    c. Another employee must be able to take over and provide the inspector with the requested information
    d. The company can submit the documents by email within 5 working days

4. Which of the following is NOT something an inspector may ask during an AML inspection?
    a. To explain why you accepted a specific counterparty
    b. To show your AML certificate
    c. To demonstrate that you have reported suspicious transactions to the CFI when required
    d. To provide a list of all transactions above €1,000 for the past 10 years

Annex A – Risk scorecard: general risk assessment on company level and actions to be taken

	The director(s) of the diamond trader has/have blank criminal record.	
	The diamond trader recently had an inspection by the FPS Economy concerning the implementation of the anti-money laundering law in his company, without any consequences.	Feedback about the inspection can be obtained at the FPS Economy.
	The diamond trader always does a notification to the CFI when he encounters a suspicious transaction or fact which could possibly relate to ML/FT.	CFI contact details: Email: info@ctif-cfi.be of Tel. 02 533 72 11
	The diamond trader applies the recommendations from the AWDC '*Best practice guide for trade in the Belgian diamond sector*'.	
	The diamond trader complies with this anti-money laundering policy.	
	The diamond trader uses the KYCP platform.	The diamond trader can demonstrate this on the basis of the list of onboarded clients/suppliers in KYCP
	The diamond trader applies the recommendations in the AWDC guide '*Sanctions and embargoes compliance guide for the diamond trade*'.	
	The diamond trader is part of a group and all entities of the group apply a similar anti-money laundering policy.	
	The diamond trader annually has many new clients/suppliers and/or a client/supplier portfolio that changes regularly.	
	One or more directors of the diamond trader have had a bankruptcy in the past.	
	The diamond trader regularly does business with countries with less supervision on the banking industry and/or a favorable fiscal regime / or countries with high risk on ML/TF	Check the following links for information about countries: https://index.baselgovernance.org/ https://www.transparency.org/cpi2018 http://www.fatf-gafi.org/countries/#high-risk https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/
	The diamond trader regularly has discussions at Diamond Office about the value of his imported or exported goods.	
	The diamond trader regularly receives or does money transfers from or to countries with less supervision on the banking industry and/or a favorable fiscal regime.	
	A part of the client/supplier portfolio of the diamond trader refuses to provide identification information and documentation about themselves/their company.	

	The diamond trader regularly receives or does payments (related to diamond transactions) in cash in countries where there are no or limited cash limits.	
	The diamond trader has a complex or untransparent company structure.	
	The diamond trader sells diamonds through the internet or through online platforms.	
	The diamond trader regularly does business with countries with countries to which sanctions or embargoes apply and/or countries which are not member of the Kimberley Process.	The diamond trader follows the *'Sanctions and embargoes compliance guide for the diamond trade'* and assesses whether, despite the high risk, it is nonetheless possible to do business, in case certain risk mitigating measures are taken. http://www.fatf-gafi.org/countries/#high-risk https://www.transparency.org/cpi2018 https://www.kimberleyprocess.com/en/kp-participants-and-observers
	The diamond trader is not registered at the FPS Economy, or his registration was suspended or cancelled.	

Annex B – Risk scorecard for accepting individual client or supplier relationships and actions to be taken

	No risks were detected via the GRID screening tool in the KYCP platform.	
	The counterparty understands the anti-money laundering legislation or similar legislation in his country and actively cooperates to provide the diamond trader all required information.	
	The counterparty is located in a EU member state, or a country outside of the EU with an effective anti-money laundering regime.	
	The diamond trader received positive references about the counterparty.	
	The counterparty is RJC (Responsible Jewellery Council) certified.	https://www.responsiblejewellery.com/members/
	The counterparty is member of a recognized diamond bourse.	The diamond trader asks for the bourse membership card.
	The counterparty is resident of a country with less supervision on the banking sector and/or a favorable fiscal regime and/or a country with a failing anti-money laundering regime/ a conflict affected and high risk area	The diamond trader undertakes the following: • obtains permission of the senior management staff in his company to conclude the business relationship and/or to execute the transaction; • gathers information about the client and its ultimate beneficial owner(s), about the intended nature of the business relationship, about the source of the funds used and the source of the client's wealth and that of its ultimate beneficial owner(s), about the reasons for the intended transactions or the executed transactions; • enhances his supervision of the business relationship;

	The counterparty has or seems to have little experience in the diamond sector.	The diamond trader asks the counterparty what kind of business relationship of or sort of occasional transaction he intends to have
	The counterparty works through one or several intermediary(ies) and/or the diamond trader has never met the client personally and it is also not clear which role the intermediary(ies) play(s) exactly.	- The diamond trader insists on meeting the counterparty personally and asks for clarification about the involvement of the different parties. - If the counterparty is a high-net-worth individual (HNWI, a person with large capital), the diamond traders asks a bank statement of this person.
	The diamond trader has had bad experiences with the client in the past (suspicion of money laundering, financing of terrorism).	
	The counterparty went bankrupt in the past and recently established a new company.	The diamond trader asks for the reasons of the previous bankruptcy.
	The counterparty is located in a country which is not a member of the Kimberley Process.	https://www.kimberleyprocess.com/en/kp-participants-and-observers The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.
	The counterparty requests you not to analyze his identity, insist on anonymity, and/or is prepared to pay/compensate for this.	The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.
	The counterparty is/was persecuted for certain serious crimes, such as money laundering, financing of terrorism, fraud.	The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.
	The counterparty is on a sanction list.	The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.
	The counterparty is a Belgian diamond trader/broker not registered at the FPS Economy.	The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.

		• makes sure that at least the first transaction is executed via an account on the client's name with a credit institution where the vigilance measures towards clients are not less strict than the principles established as per the anti-money laundering law. The source of the funds can possibly be checked by asking confirmation to the client that his financial resources stem from the ordinary operating funds of the company. Also pay checks, tax declaration documents, independent audit reports or media reports could provide information on this. Check the following links for information about countries: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_en https://index.baselgovernance.org/ https://www.transparency.org/cpi2018 http://www.fatf-gafi.org/countries/#high-risk https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/ https://www.cahraslist.net/cahras
	The ownership structure of the company of the counterparty seems unusually or excessively complex considering the type of company activity.	The diamond trader requests to provide a clear structure or organizational chart of the company, if applicable with the shareholder registers or other pieces of evidence which can demonstrate the identity of the ultimate beneficiaries.
	The diamond trader never met his counterparty personally.	
	Negative media is connected to the counterparty	
	The counterparty is a politically exposed person (PEP), family member of a PEP or close associate of a PEP.	The diamond trader takes extra vigilance measures for clients who are PEPs, family members of close associates thereof. In any case he takes the following measures: o He obtains permission of the higher management in the company to enter into or continue the business relationship with these persons; o He takes appropriate measures to determine the origin of the funds which are used in the business relationship or transactions with these persons; o He exercises a stricter supervision on the business relationship and the execution of the transaction.
	The identification details which the counterparty has provided, do not correspond to information which one finds through certain verification tools.	The diamond trader asks additional documents to verify the identity of his client or supplier.
	The identification details which the counterparty provided, are not official, do not look authentic or are not up-to-date.	The diamond trader asks additional documents to verify the identity of his client or supplier.
	It is unclear what type of business relationship/occasional transaction the counterparty wants.	The diamond trader asks the counterparty what kind of business relationship of or sort of occasional transaction he intends to have.
	The counterparty is active in a sector where the purchase or sale of diamonds does not logically fit in its corporate purpose (e.g. a sector other than diamond trade, jewelry,...)	The diamond trader pays attention if the sector in which the counterparty is active is a high-risk sector such as second-handed vehicles, construction, ...

Annex C – Risk scorecard for monitoring during business or occasional relationship

	The counterparty executes payments and/or invoices in accordance with the AWDC *'Best practice guide for trade in the Belgian Diamond sector '.*	Where appropriate, the diamond trader insists with the counterparty to follow the recommendations in this guide.
	The flow of goods which relate to transactions with a counterparty outside of the European Union are being controlled by the Belgian Diamond Office.	This is a legal obligation
	The counterpary pays from a country with less supervision on the banking sector and/or a favorable fiscal regime and/or with a high money laundering and/or corruption risk and/or countries for which sanctions/embargoes apply and/or countries which are not member of the Kimberley Process.	The diamond trader will monitor these transactions even more closely, check the origin of the funds and see whether these are consistent with the individual risk analysis made of the client.
	The seller's invoice does not clearly indicate whether it concerns synthetic/treated diamonds or (natural) diamonds.	The diamond trader follows the recommendations of the AWDC *'Best practice guide for trade in the Belgian diamond sector '.*
	The counterparty often changes his bank account.	The diamond trader asks his counterparty to explain.
	The client wants to pay through a currency broker, money transfer services (MoneyGram), Hawala or payments in new digital coins (e.g. Bitcoin).	The diamond trader follows the recommendations of the AWDC *'Best practice guide for trade in the Belgian diamond sector'.*
	The counterparty suggests an atypical payment/delivery method (e.g. payment through a third party, payment through the account of a third party, payment through other channels than official banks/financial institutions is proposed).	The diamond trader asks the counterparty to explain. He checks the origin of the funds and whether these are consistent with the individual risk analysis made of the client. Where appropriate, he makes a tripartite agreement as recommended in the AWDC *'Best practice guide for trade in the Belgian diamond sector'.*
	The counterparty wants to execute a complex or unconventionally big transaction with does not have a visible economic or legitimate purpose.	The diamond trader checks the origin of the funds and whether these are consistent with the individual risk analysis made of the counterparty. He asks his counterparty to explain and follows the recommendations of the AWDC *'Best practice guide for trade in the Belgian diamond sector'.*
	The client insists on cash payments of more than 3,000 Euros in Belgium.	The diamond trader does not execute the transaction and notifies the CFI.
	The supplier of the diamond trader cannot provide a Kimberley Process Certificate for the delivery of rough diamonds or it concerns a rough transaction from a country that is not member of the Kimberley Process.	The diamond trader does not execute the transaction and notifies the CFI.

TOOLS TO HELP COMPLY WITH AML

AWDC

KYCP	MYAWDC
Identifying & verifying counterparties	Watch AML seminar + acquire AML certificate
Risk assessment	Watch Best Practices seminar + acquire Best Practices certificate
Updating AML information	Consult invoices
Screening tool access: ORBIS & GRID	Consult G7 & GF certificates
	Consult customs documents & track shipments

QUESTIONS?
CONTACT AWDC HELPDESK
Tuesday, Wednesday & Thursday (10am - 1pm)
helpdesk@awdc.be

FPS ECONOMY

DIAMOND SUPERVISION
Submit AML report
Consult previous AML reports
Submit stock declaration
Consult public list of registered diamond companies
Submit KP declarations

QUESTIONS?
CONTACT FPS ECONOMY
diamond@economie.fgov.be
02 277 54 59

AWDC

The AML Journey

1 Organisational Obligations

Have internal AML policy
Appoint min. 1 AML officer
Pass online AML quiz yearly or physical AML exam 3-yearly
Submit annual AML report to FPS Economy

2 KYC (Know Your Counterparty)

Collect AML related info about counterparty before establishing relationship
Verify, keep up-to-date, and store properly
→ Know who you're doing business with to manage risks

3 Risk Analysis

Based on KYC, assess safety of doing business with this party
Use risk scorecards to assign risk category (low, medium, high)
Keep info up-to-date

4 Make a Decision

Accept the business relationship
OR
Accept under certain conditions
OR
Refuse or terminate the business relationship

5 Reporting Suspicious Situations

Identify suspicious situations
Report unusual of suspicious actions, even without proof, to CFTI
Protect your company and contribute to reputation of Antwerp's diamonds