Ensuring Compliance – Notes from the Enforcement Section for the Gaming Sector

Dr Stephanie Camilleri and Dr Christabel Coleiro

FIAU - Enforcement Section

The AML/CFT Gaming Conference - 29th September 2023

Legislation, Administrative Measures and the Enforcement Process

Legislation

The **FIAU** is empowered to enforce the provisions found under the:

i. **Prevention of Money Laundering Act (PMLA)**

ii. **Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR)**

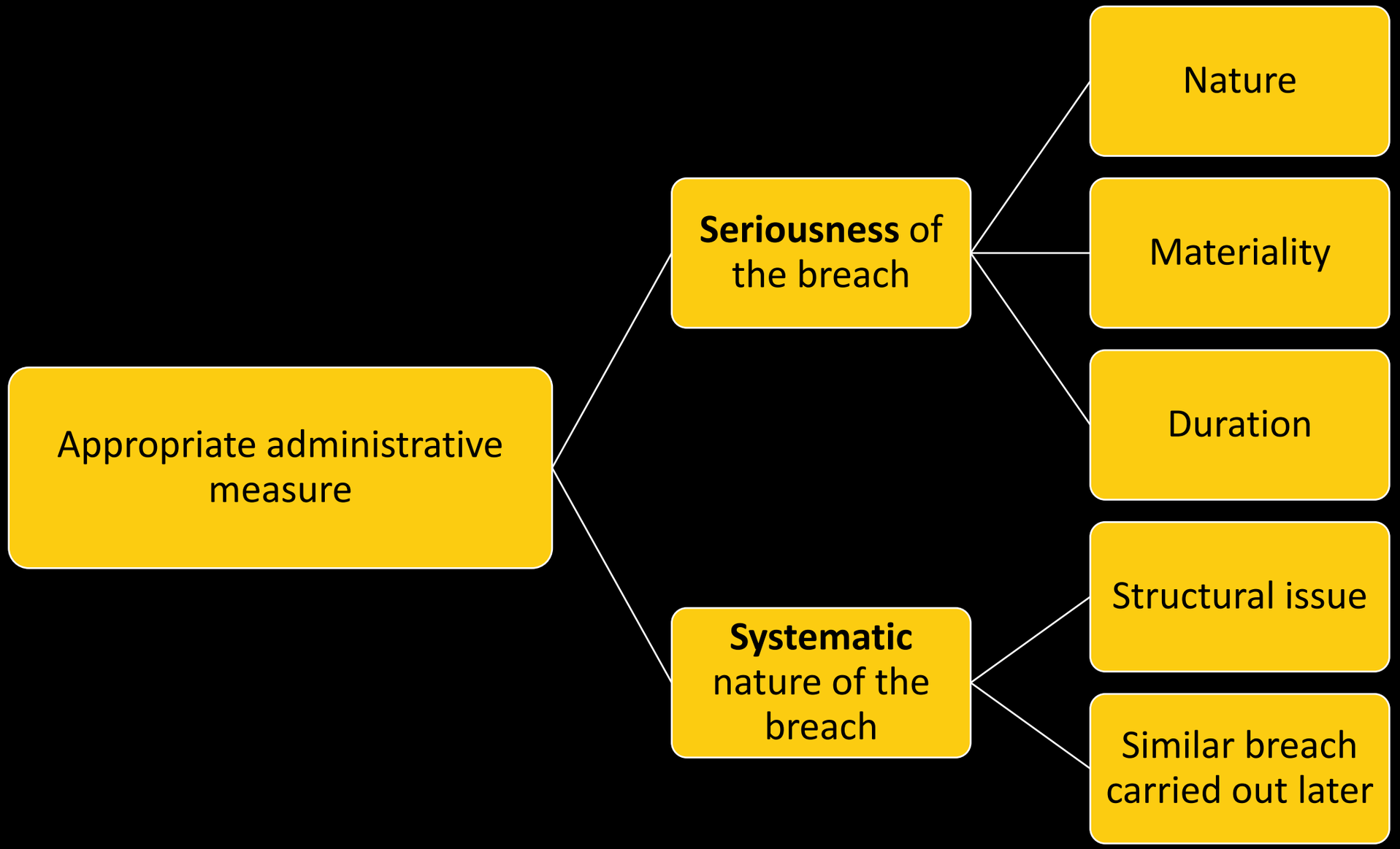
iii. Any **procedure** or **guidance** issued in terms of the PMLFTR

through the imposition of Administrative Measures for identified breaches of AML/CFT obligations in terms of the FIAU's powers envisaged under:

i. **Regulation 21** of the **PMLFTR**

ii. **Article 30C** of the **PMLA**

Aggravating/Mitigating Factors



Aggravating/Mitigating Factors

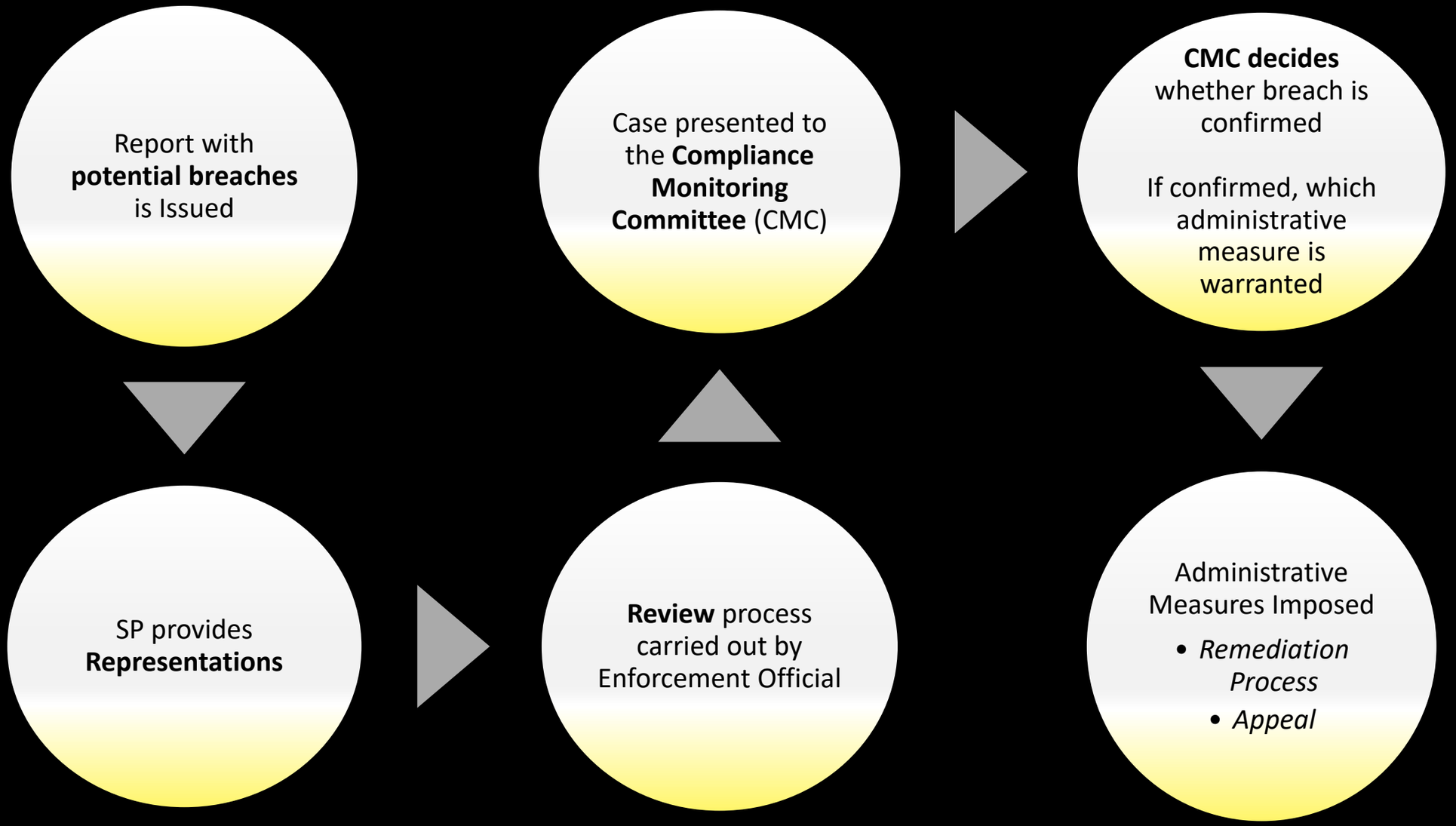
Other factors taken into consideration:

- the **size** of the SP
- the **repercussions** which a breach may have on the jurisdiction
- how the breach had **facilitated** ML/FT

Administrative Measures

Administrative Penalties	→	**Repeated/serious/systematic (or a combination thereof) breach**
Directives	→	**Remediation/Follow-Up**
Written Reprimand	→	**No significant consequences caused**

Enforcement Process

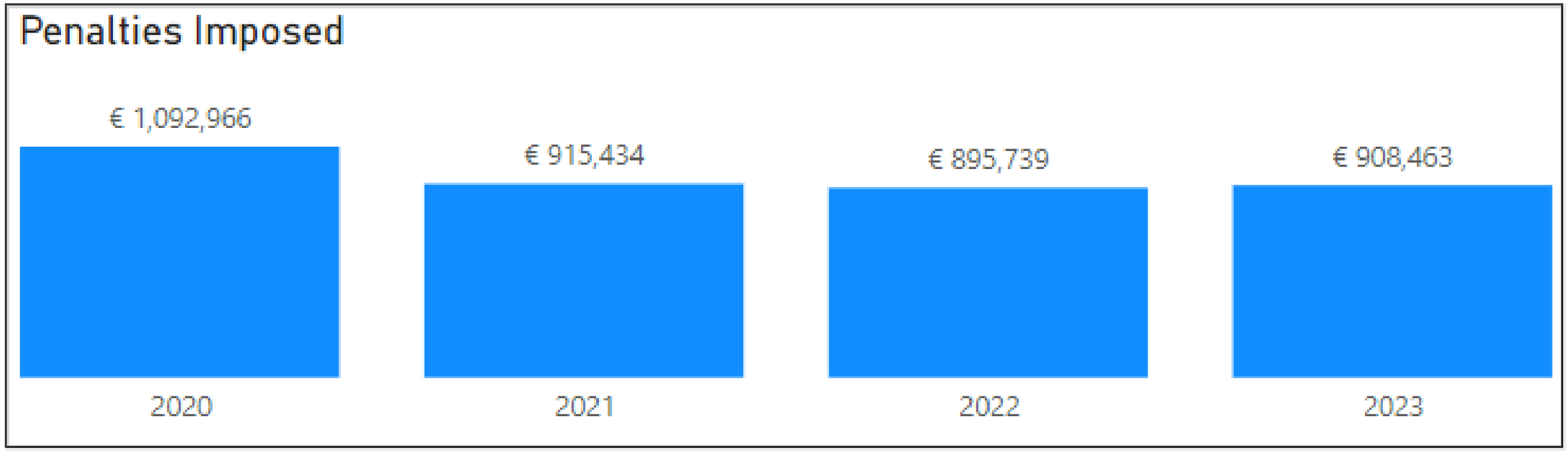


Administrative Penalties Imposed on Gaming Companies (including Land Based Casinos) – data as at 31 August 2023

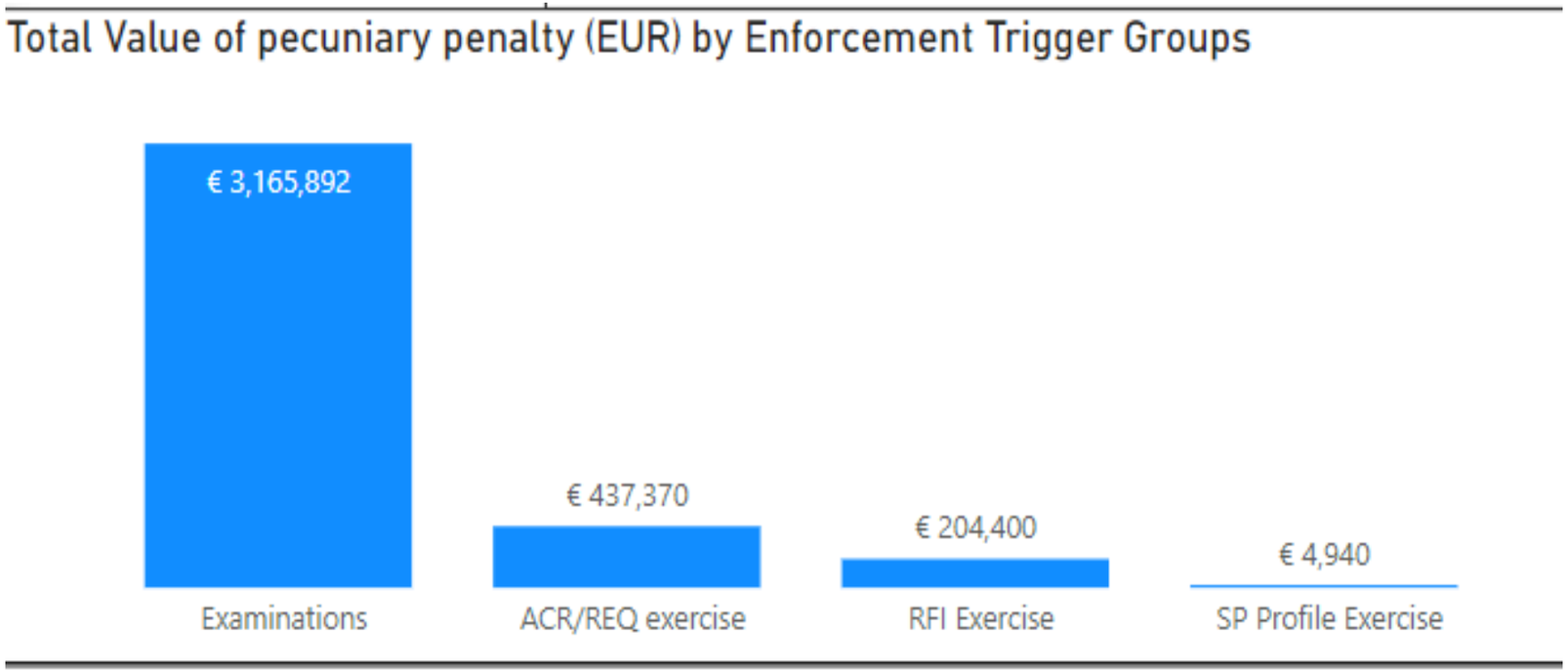
Year of Sanction

2020 | 2021 | 2022 | 2023

No. of SPs Sanctioned	No. of Sanctions Imposed	Amount of Penalties
155	215	€ 4M



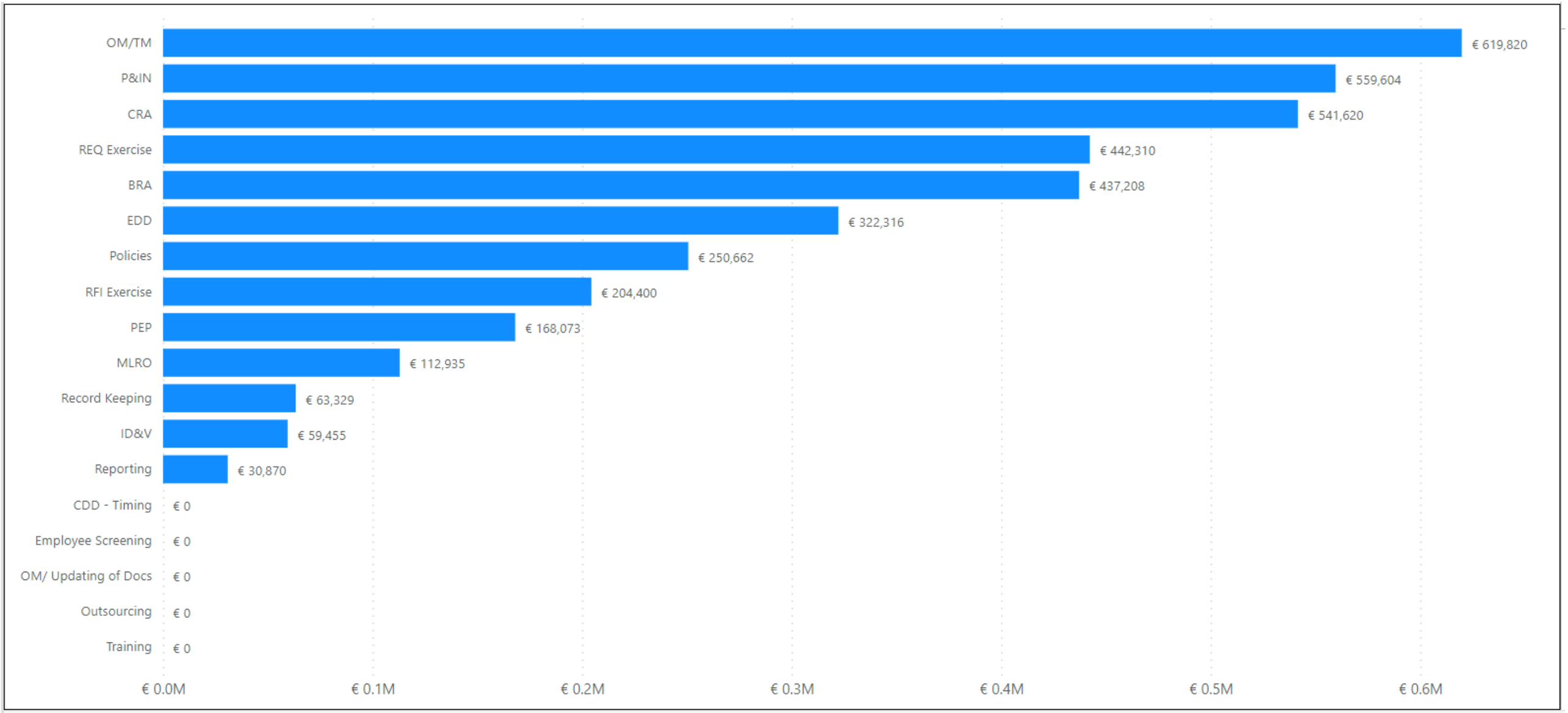
Administrative Measures Imposed on Gaming Companies (including Land Based Casinos) – data as at 31 August 2023



Sanctions by Trigger by Year

Trigger	2020	2021	2022	2023	Total
RFI Exercise			69	40	**109**
ACR/REQ exercise	52	16	8	11	**87**
Examinations	2	4	4	6	**16**
SP Profile Exercise			3		**3**
Total	**54**	**20**	**84**	**57**	**215**

Administrative Measures Imposed on Gaming Companies (including Land Based Casinos) – data as at 31 August 2023



Legal Obligations and Main Breaches Identified

Business Risk Assessment

- **Section 3.3.2 of the IPs Part I** → all aspects of the BRA are to be documented and evidenced including:

a) The **methodology** adopted to conduct the assessment;

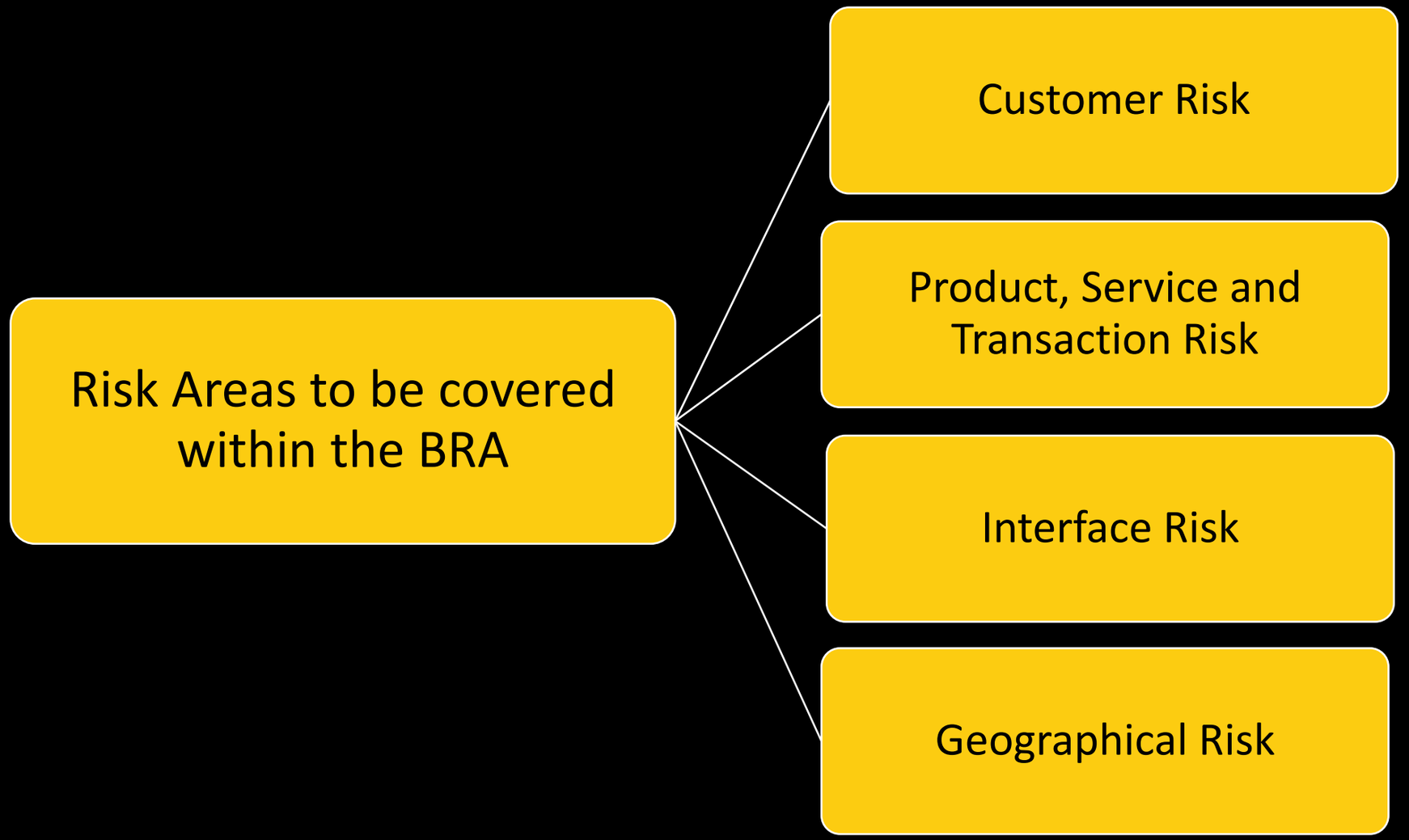
b) The **reasons** for considering a risk factor as presenting a **low**, **medium** or **high risk**;

c) The outcome of the BRA;

d) Any **information sources** used.

- BRA shall be **revised** whenever there are changes within the business structure/activities.

Business Risk Assessment



Business Risk Assessment – Breaches Identified

- BRA failed to **consider all of the four Risk Pillars comprehensively**
- BRA failed to include **quantitative data in determining the likelihood** of risks materialising
- BRA failed to provide an evaluation of the **strength of mitigating measures** with respect to each risk scenario identified.
- The mitigating measures mentioned in the BRA are the same for all risks identified.
- BRA failed to include **pertinent risks which are applicable to the modus operandi** of the Company.
- BRA failed to provide the **overall resulting inherent and residual risk ratings**.

Customer Risk Assessment

Section 2.1.1 IPs Part II:

- CRA is required in order to:

i. **Identify potential risks** upon entering a business relation with, or carrying out an occasional transaction for, a customer;

ii. Develop **a risk profile** for the customer and **categorise the ML/FT risk** posed by such customer as **low, medium** or **high**;

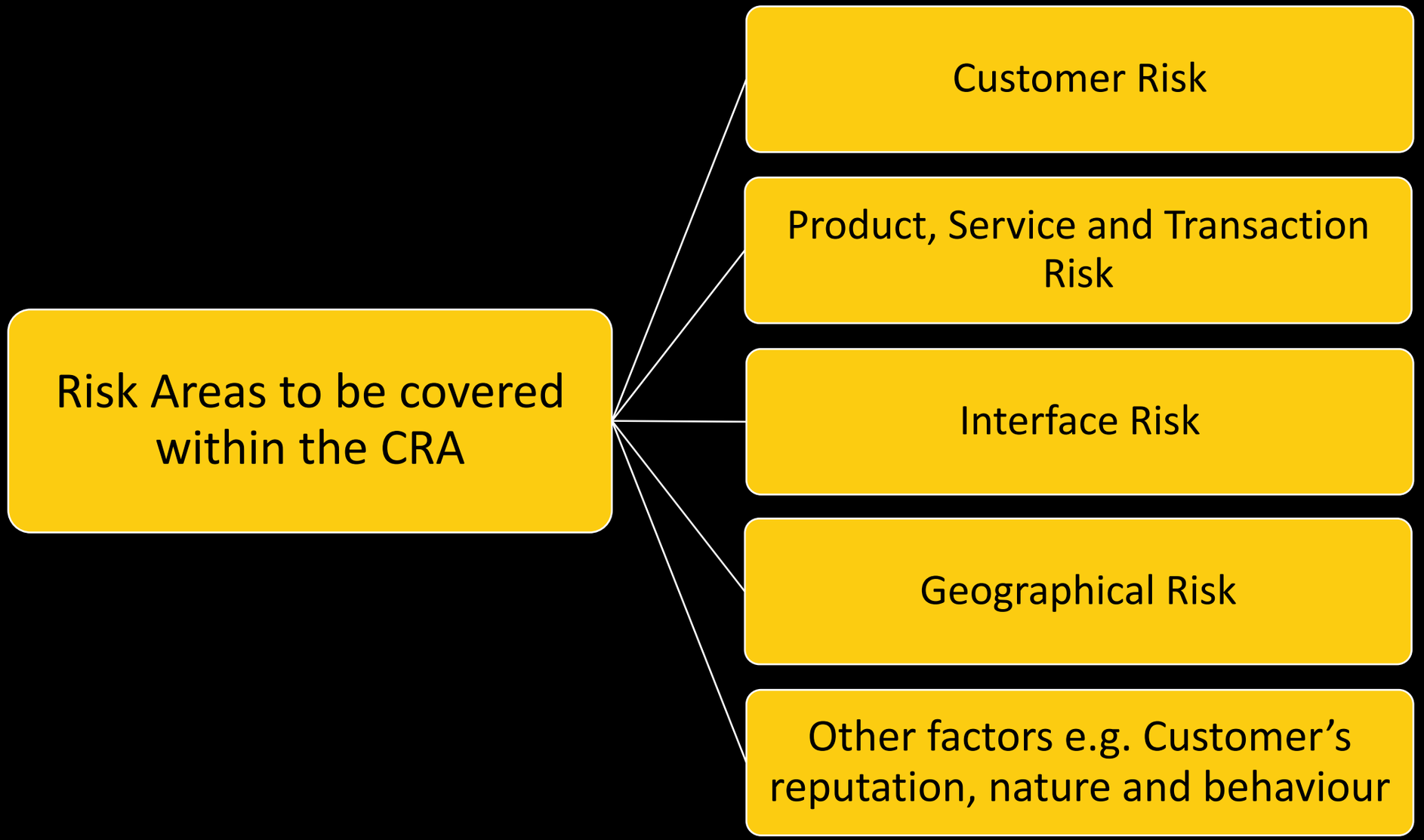
Section 2.2.1 IPs Part II:

- CRA is to be carried out either:

i. **Prior** to the carrying out of an occasional transaction; or

ii. In the case of a business relationship, **not later than 30 days** from when the €2,000 deposit threshold is reached.

Customer Risk Assessment



Customer Risk Assessment – Breaches Identified

- **No CRA** carried out for customers who had **exceeded** the €2,000 deposit threshold
- Customers' risk rating **not re-assessed** upon hitting the €2,000 deposit threshold
- CRAs carried out **after the lapse of 30 days** from when the €2,000 deposit threshold was reached.
- CRA **methodology** does not take into consideration all factors which could potentially pose a ML/FT risk to the SP

Customer Due Diligence

Aim of CDD

Build a **customer profile** on the basis of which the **customer's activity** can be assessed to identify any **unusual behaviour**.

Customer Due Diligence

- **Regulation 9(1) PMLFTR:**

  Casino and gaming licensees shall apply customer due diligence measures when carrying out transactions that amount to or exceed two thousand euro (€2,000) or more, whether carried out within the context of a business relationship or otherwise.

- **Section 2.1 of the IPs Part II (Land-Based Casinos)**

  Casino licensees are expected to conduct CDD:

  a) When a person enters the premises of the casino

  b) When a person, while at the casino, purchases from the casino or exchanges at the casino, chips or tokens for the value of €2,000 or more;

  c) When a person, while at the casino, carries out an occasional transaction of €15,000, or more; and

  d) When a person seeks to establish a business relationship.

CDD – Identification & Verification

- **Section 4.3.1 of the IPs Part I** and **Section 3.2 of the IPs Part II –**

  Standard identification procedure consists in the gathering of the following personal details:

  (a) Name and surname;

  (b) Permanent residential address;

  (c) Date of birth;

  (d) Place of birth;

  (e) Nationality; and

  (f) Identity reference number where applicable.

Identification & Verification – Breaches Identified

- Failure to identify the customers' **place of birth** and **permanent residential address**
- Failure to obtain documented evidence in order to **verify the customers' identity** and **residential address documents within 30 days** of reaching the €2,000 deposit threshold

CDD – Purpose and Intended Nature

Low Risk Customers	No detailed SoW information required; it is sufficient for the customer to declare his employment details.
Medium Risk Customers	SoW is to be obtained unless the SP opts to consider using statistical data to develop behavioural models against which the customer's activity can be determined.
High Risk Customers	SoW information has to be obtained and this needs to also be supported by independent and reliable documentation.

CDD – Purpose and Intended Nature

- Gaming/Casino licensees are expected to gather information on:

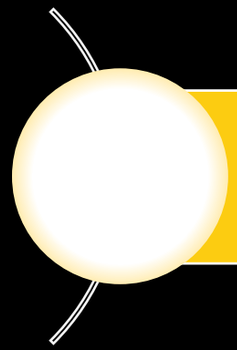
a) The **nature** and **details** of the **business/occupation/employment** of the customer;

b) The **source(s) of wealth**;

c) The **expected source and origin of the funds** to be used in the business relationship; and

d) The **anticipated level and nature of the activity** that is to be undertaken through the relationship.

Purpose and Intended Nature – Breaches Identified



No **SoW/SoF** information obtained from **medium** and/or **high-risk** players. In the case of medium risk players neither was any statistical data obtained

Enhanced Due Diligence

- **Regulation 11 PMLFTR**

EDD shall be applied :

a) In relation to activities or services that are determined by the FIAU to represent a high risk of ML/FT, having taken into consideration the findings of any national risk assessment and any other relevant factors, as may be deemed appropriate.

b) Where, on the basis of the BRA the subject person determines that an occasional transaction, a business relationship or any transaction represents a high risk of ML/FT.

c) When dealing with natural or legal persons established in a non-reputable jurisdiction other than branches or majority-owned subsidiaries which comply with group-wide policies and procedures. In relation to such branches or majority-owned subsidiaries EDD is to be applied when these present a high risk of ML/FT.

Enhanced Due Diligence

With respect to the **gaming industry** high risk scenarios also include:

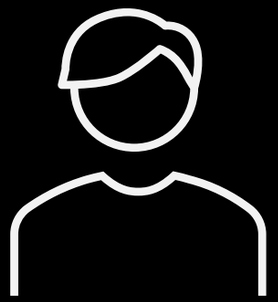
- large value and volume of gameplay
- the payment methods being used by the customer
- the use of multiple payment methods.

Enhanced Due Diligence

- Section 3.2 of the IPs Part II

Where the amounts deposited by a customer are particularly large, even if these amounts may be in line with the customer's profile, the licensee is still obliged to carry out enhanced monitoring on the same to meet its obligations at law. This includes obtaining independent and reliable information and documentation on the source of wealth and source of funds used by the customer to fund the particularly large transactions.

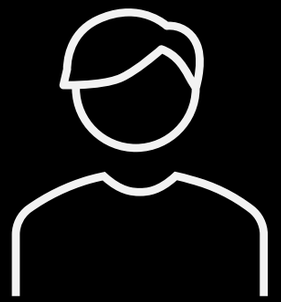
EDD – Case Studies



Player 1

- €2,000 deposit threshold reached following a month from registration;
- Monthly salary ranging between €750 and €1,000;
- €100,000 deposited within the following 3 months;
- €25,000 deposited via **prepaid cards** and €3,000 via **Skrill**.

EDD – Case Studies



Player 2

- Player was unemployed;
- €400,000 dropped within 3 years mostly in cash;
- €175,000 lost;
- Player was first attributed a low-risk rating which was subsequently raised to high risk;
- No background checks carried out.

Transaction Monitoring

- **Section 4.5.2.1 – Purpose of Transaction Monitoring**

Through the monitoring of customer transactions or activities, subject persons should be in a better position to:

(a) identify behaviour or transactions that diverge from the usual pattern of transactions, do not fit within the customer's profile, or are otherwise not in line with what is normally expected from the customer, and which therefore need to be questioned in further detail

(b) identify suspicious activity in relation to which an STR is to be filed with the FIAU; and

(c) determine whether the initial risk assessment requires updating, and whether, in view of the updated risk assessment or other considerations, the business relationship remains within the subject person's risk appetite and, if so, understand whether the level of CDD needs to be adjusted in view of any changes from the initial risk understanding.

Transaction Monitoring

- **Section 3.3.2 of the IPs Part II Remote Gaming Sector:**

  Even before reaching the €2,000 threshold, licensees are to have systems in place which allow them to apply a level of on-going monitoring. Through these systems, licensees should ensure that:

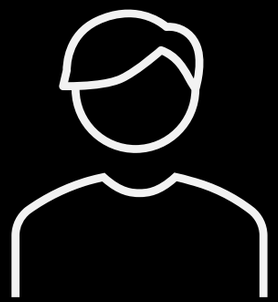
  a. They are able to determine the moment in time when the €2,000 threshold is met;

  b. The player does not avoid the application of CDD measures by circumventing the €2000 threshold;

  c. They are able to deny the application for the opening of an account by a person who has inputted manifestly false details; and

  d. They are able to detect instances which give rise to a suspicion of ML/ FT

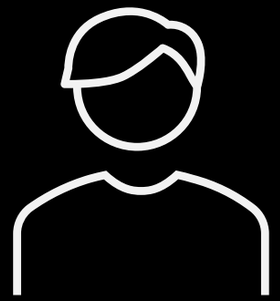
Transaction Monitoring – Case Studies



Player 1

- €5,000 deposited over 5 days;
- SoW information requested from the player a month later and the player declared a monthly income in the range of €1,500 and €2,000;
- Player was allowed to continue depositing;
- An additional €35,000 deposited;
- No SoF/SoW documentation requested.

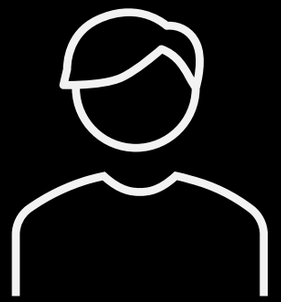
Transaction Monitoring – Case Studies



Player 2

- €10,000 deposited within 2 months;
- No SoF/SoW information obtained;
- No employment information obtained.

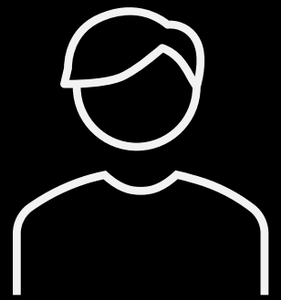
Transaction Monitoring – Case Studies



Player 3

- €10,000 deposited within a month;
- No SoF/SoW information obtained;
- €35,000 deposited within the following 4 months;
- A month later, the player was requested to provide SoF/SoW information and documentation, however the player failed to do so.

Transaction Monitoring – Case Studies



Player 4

- €20,000 deposited within a month.
- The SP only requested for the player’s information and documentation a year later, during the compliance examination.

Thank you!

Financial Intelligence Analysis Unit

Ensuring Compliance – Notes from the Enforcement Section for the Gaming Sector

Dr Christabel Coleiro

Enforcement

Corrective Actions

September 2023

Corrective Actions

Overview of the procedure followed, best practices and issues found

Overview of the Process relating to the Directives

Directives

Main aim – to ensure remedial action is taken

Overview of the Process relating to the Directives

Supervisory examination

CMC – to decide on the administrative measure to impose

Overview of the Process relating to the Directives

The process of a directive usually involves:

- The collection of an action plan
- The collection of documentation and/or information
- A review of files
- A live demonstration of the system/s utilised by the subject person

Overview of the Process relating to the Directives

We normally ask for updated policies and procedures, including:

- Business Risk Assessment
- Customer Risk Assessment
- Customer Acceptance Policy
- Procedures relating to Due Diligence, Record-Keeping and Reporting amongst others

Overview of the Process relating to the Directives

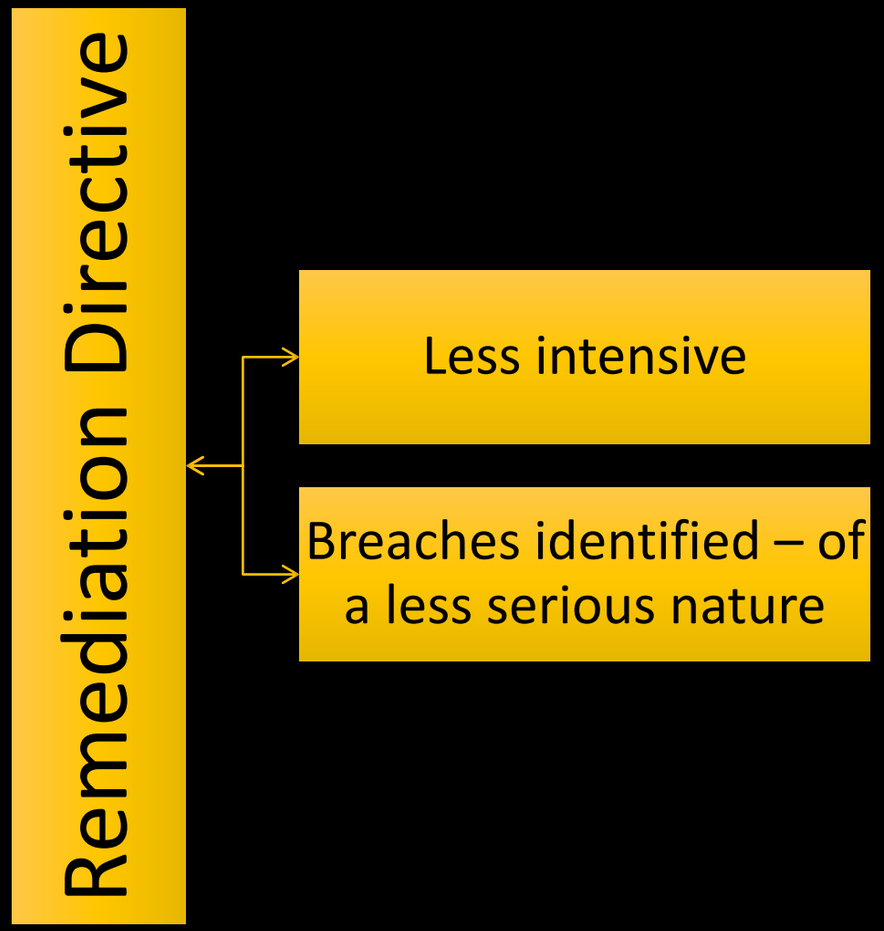
We may also ask for a sample of files

- Checking effectiveness of the subject person’s procedures

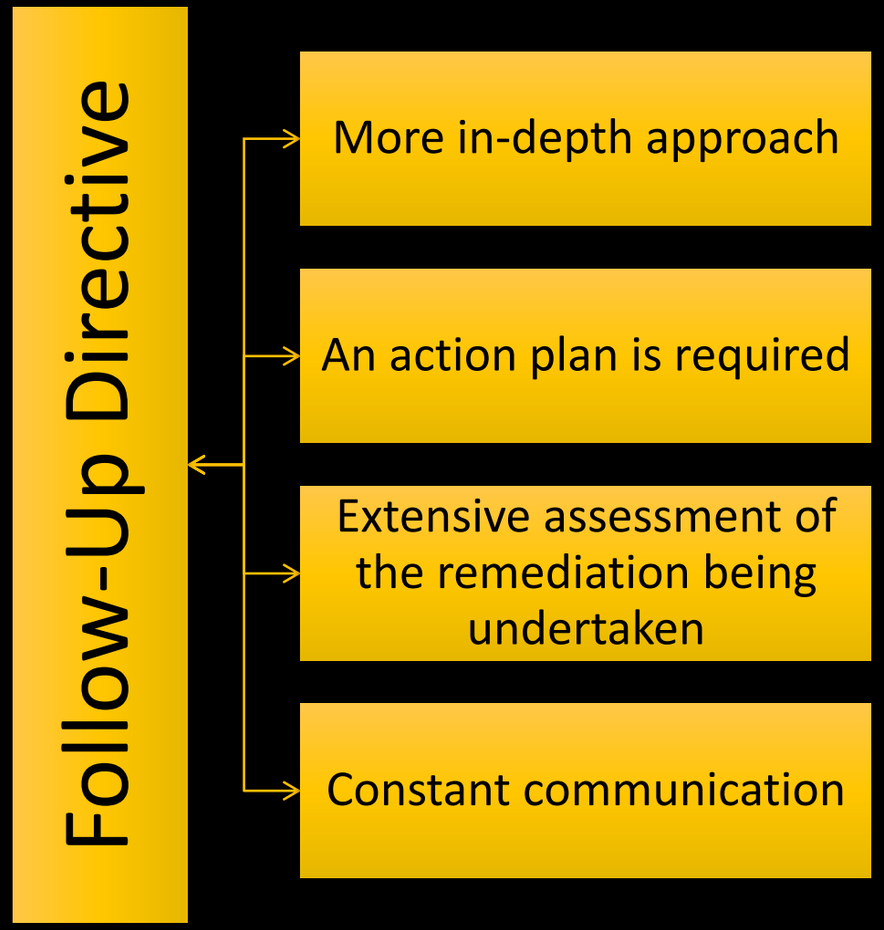
Remediation Directive vs Follow-Up Directive

- *Aim of both* – to ensure that the subject person effectively remedies its breaches at the time of the examination

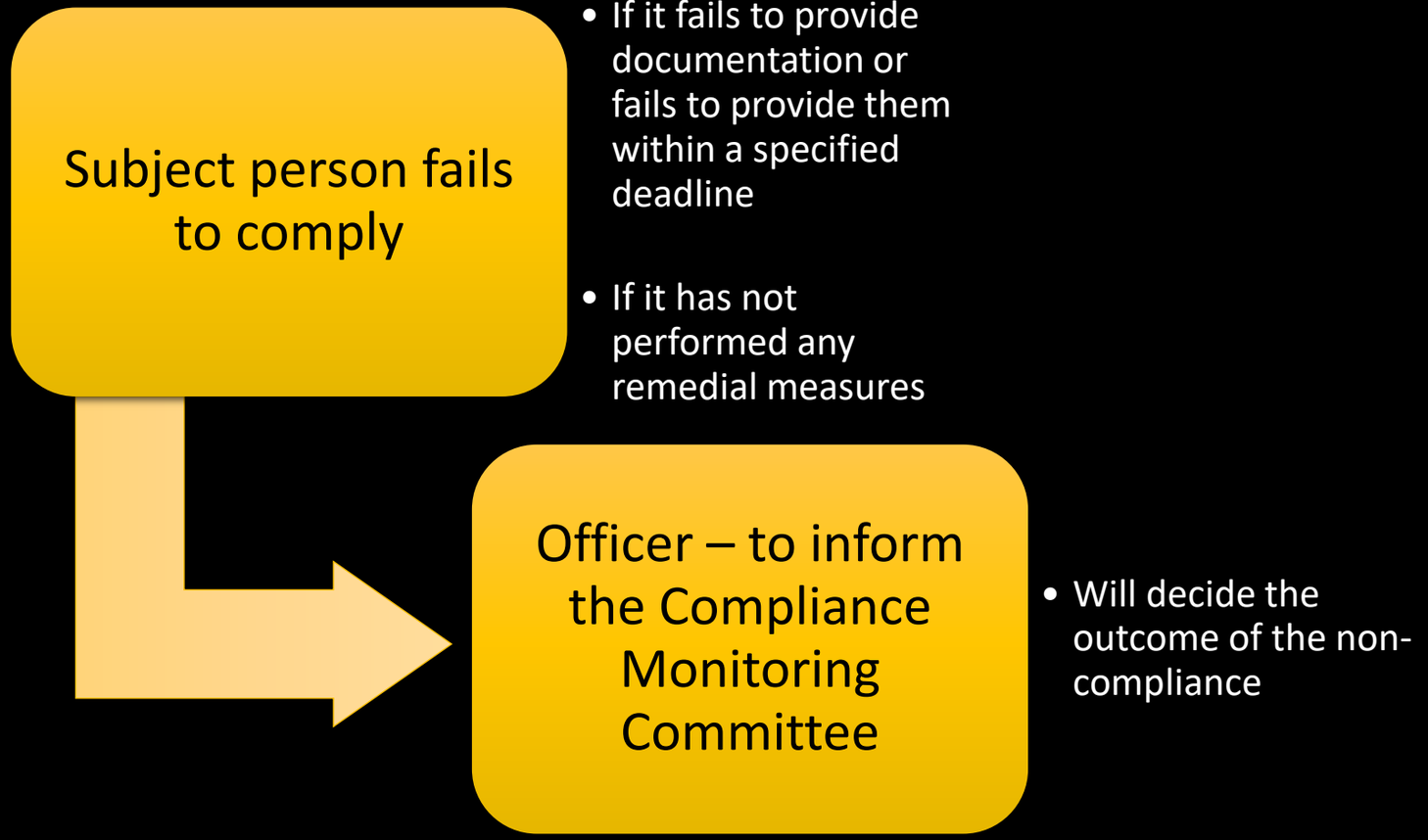
Remediation Directive vs Follow-Up Directive



Remediation Directive vs Follow-Up Directive

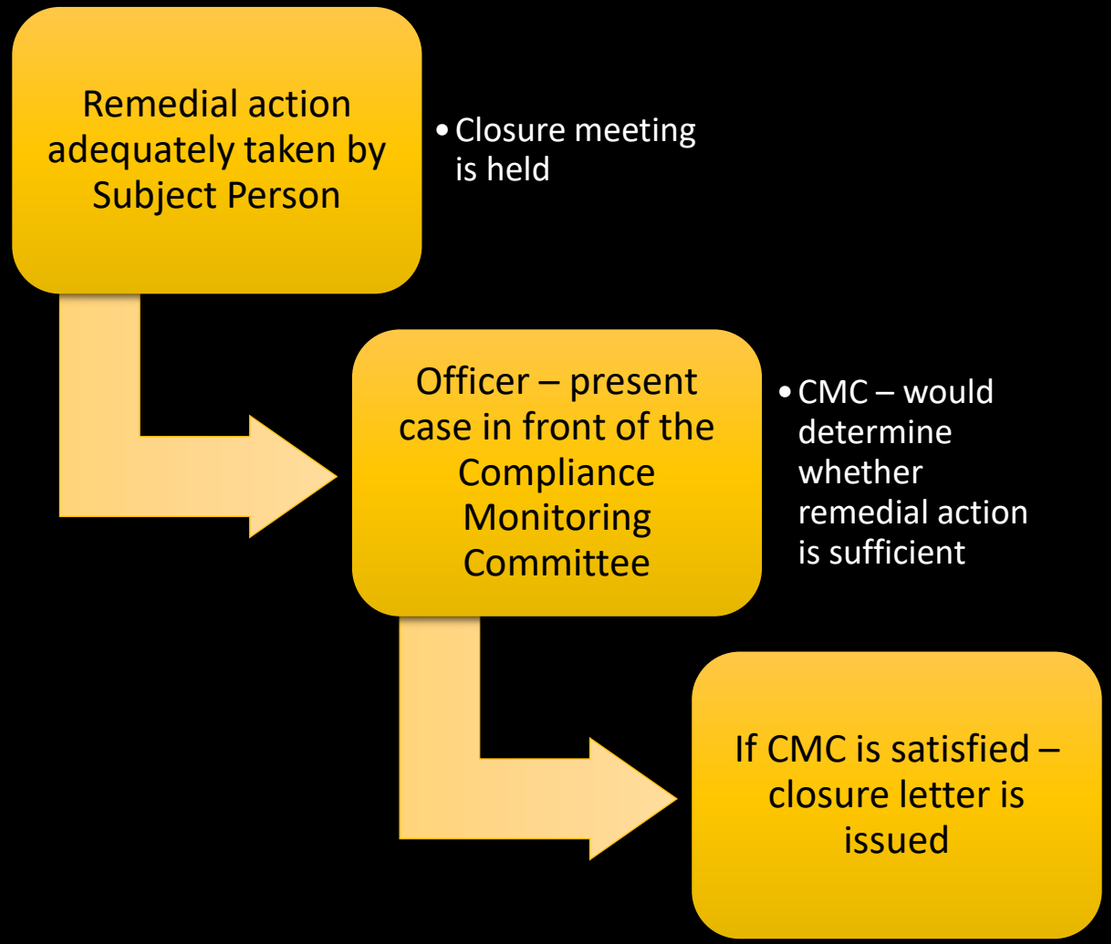


Non-Compliance with the Directive



- If it fails to provide documentation or fails to provide them within a specified deadline
- If it has not performed any remedial measures
- Will decide the outcome of the non-compliance

Compliance with the Directive

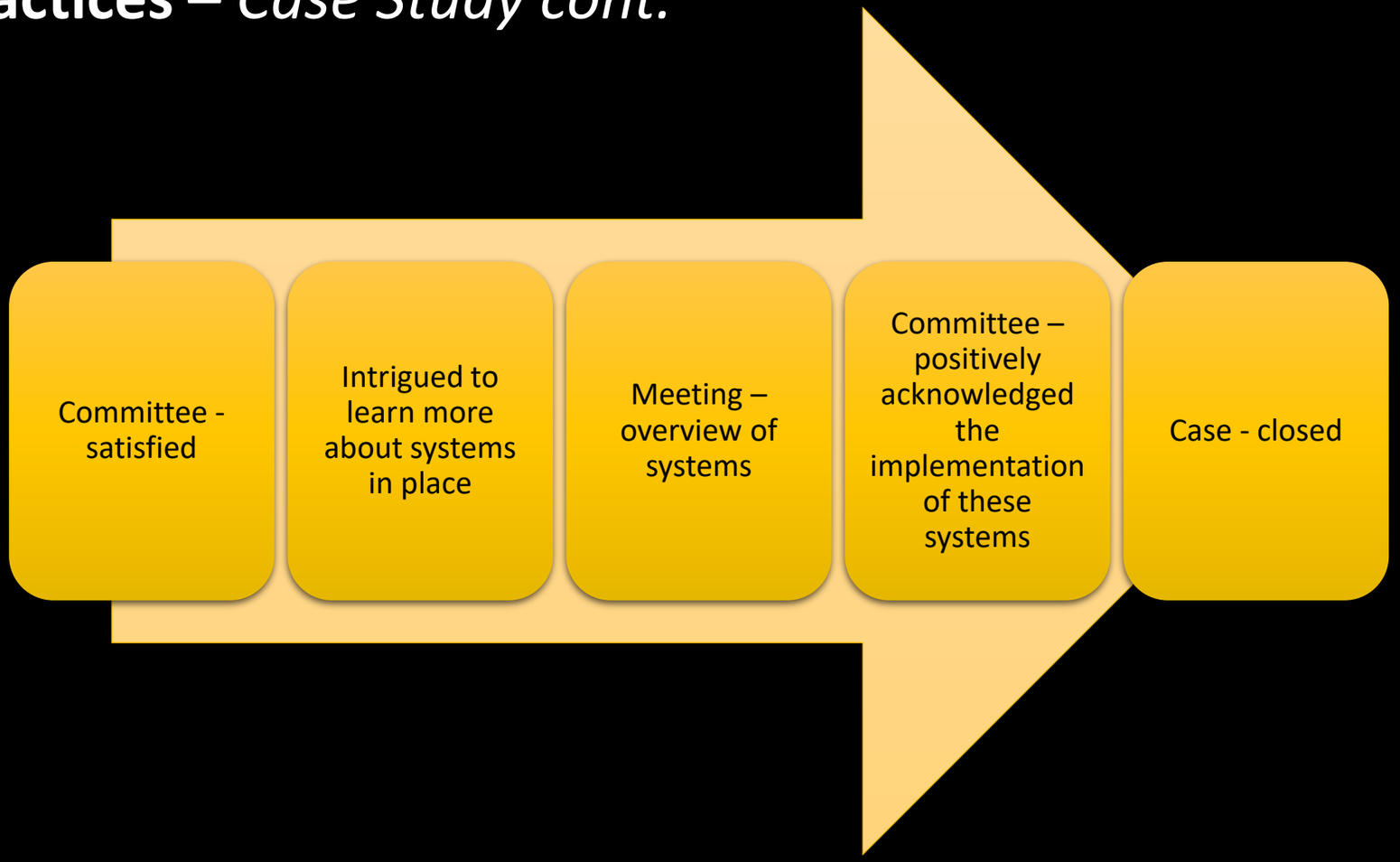


Best Practices – *Case Study*

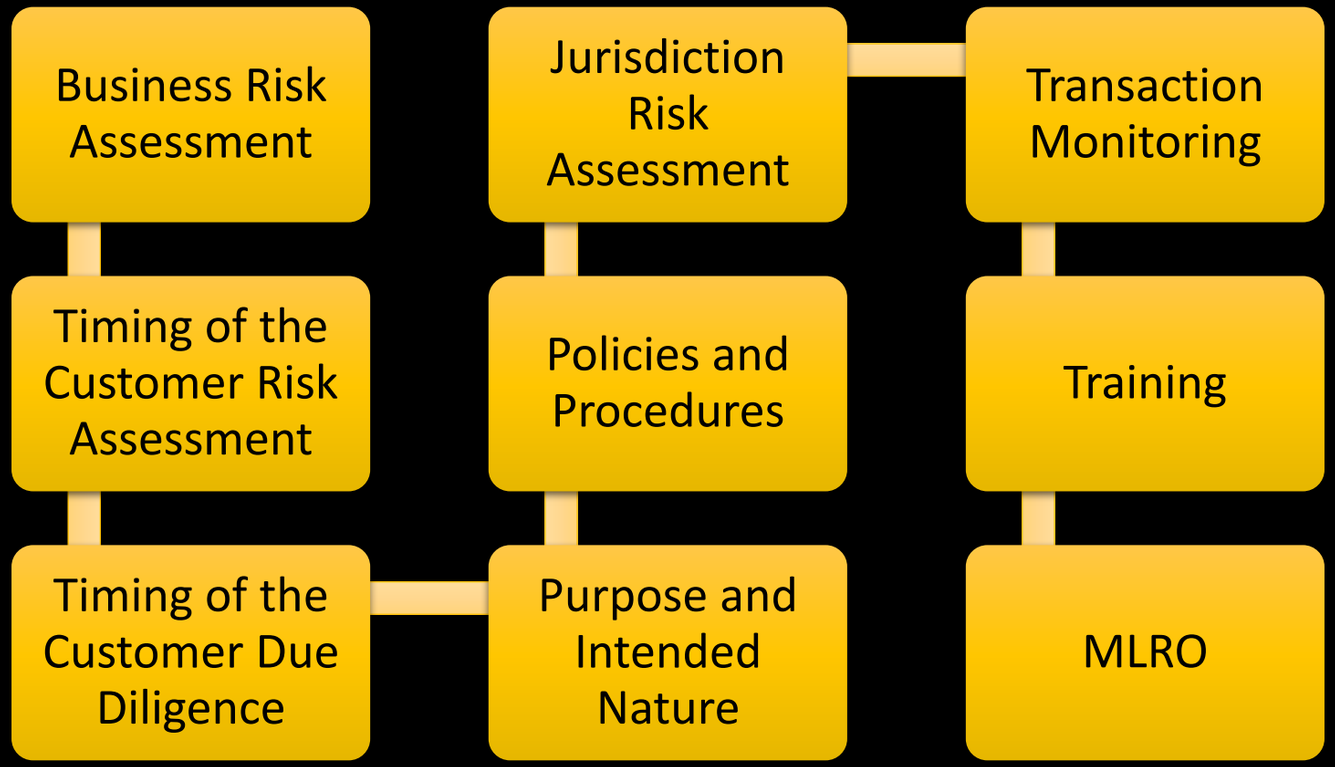
Best Practices – *Case Study cont.*

Remedial Actions

Best Practices – *Case Study cont.*



Issues noted during the remediation process



Issues with the Jurisdiction Risk Assessment Methodology

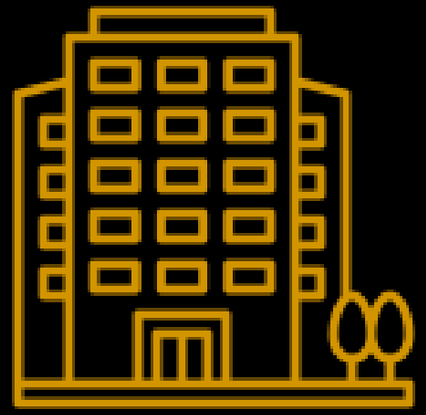
Subject Persons – to assess whether jurisdictions they are dealing with are **non-reputable** or **high-risk jurisdictions**

Required to go **beyond** the mere **identification** of non-reputable jurisdictions

Should carry out an **assessment** of certain **risk factors associated** with that **particular jurisdiction**

Assessment should be used to **evaluate and determine** the **exposure** to the **risks posed by such jurisdictions** in terms of the Company's player base

Issues with the Jurisdiction Risk Assessment Methodology – *Case Study*



Company B

Follow-Up Directive	Remediation Process	Issue
Instructed to remediate its jurisdiction risk assessment Only considered one source	Provided updated document Catered for this issue	Simply included a numerical assessment No methodology of how the Company arrived at such scorings

Issues with the Policies and Procedures

Having **adequately documented** policies and procedures – helps **mitigate or prevent ML/FT risks** from happening

Subject Persons – to ensure that the policies and procedures are then **properly applied** in their day-to-day operations

Issues with the Purpose and Intended Nature of the Business Relationship

Purpose behind opening a gaming account – **may be self-evident**

HOWEVER, it is important to ensure that **sufficient information** is collected in order to **build a comprehensive profile**

This will **help detect any abnormal** or **unusual activity**

Extent of information to be collected is determined on a **risk-based basis**

Issues with the Purpose and Intended Nature of the Business Relationship – *Case Study*

Company C

Once the EUR2,000 threshold within a 180 rolling day period is reached, players have 30 days to provide the Company with a questionnaire

Issues with the Purpose and Intended Nature of the Business Relationship – *Case Study cont.*

During the course of the remediation – still failed to obtain the required SOW/SOF information

Generic information collected

Example:

Customer X

Issues with the Transaction Monitoring System

Transaction monitoring ensures the transactions undertaken are **in line with the customer's business and risk profile**

Subject Persons are to have **effective means** to conduct **effective and adequate transaction monitoring**

Transactions can be monitored in **real time or after the event**

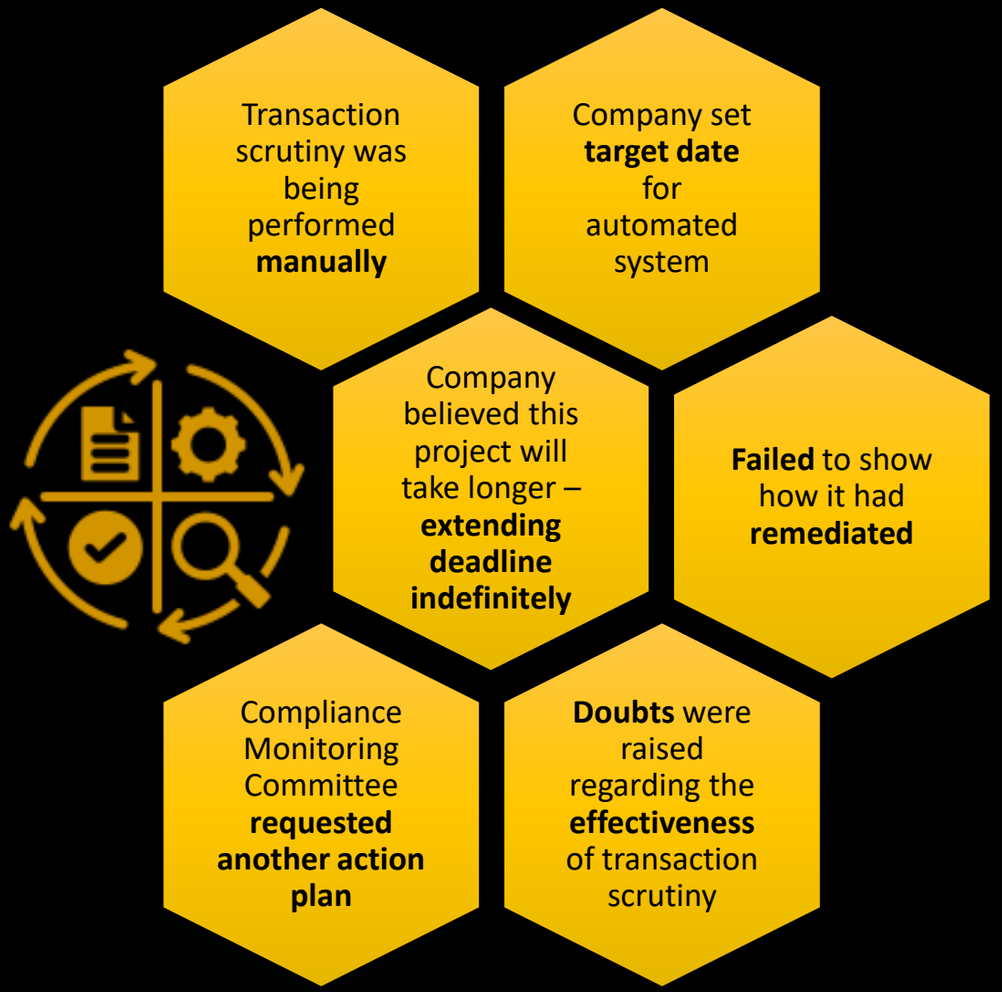
Issues with the Transaction Monitoring System – *Case Study*

Company D

Provided Action plan within stipulated deadline

Action Plan was reviewed

Issues with the Transaction Monitoring System – *Case Study cont.*



Issues with the Transaction Monitoring System – *Case Study cont.*

Manual vs Automated Transaction Monitoring

Implementing Procedures

It is **up to the subject person** to determine whether to opt for an automated or manual system

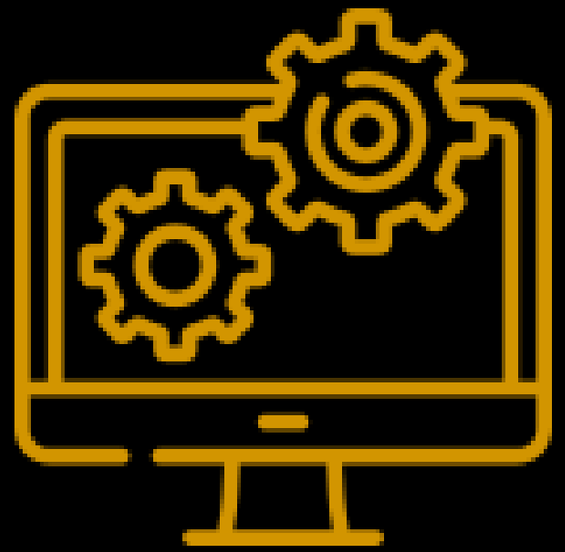
Subject Persons **need to provide** sufficient **justification** that transactions are monitored **effectively and efficiently**

Company D

High volume of customers

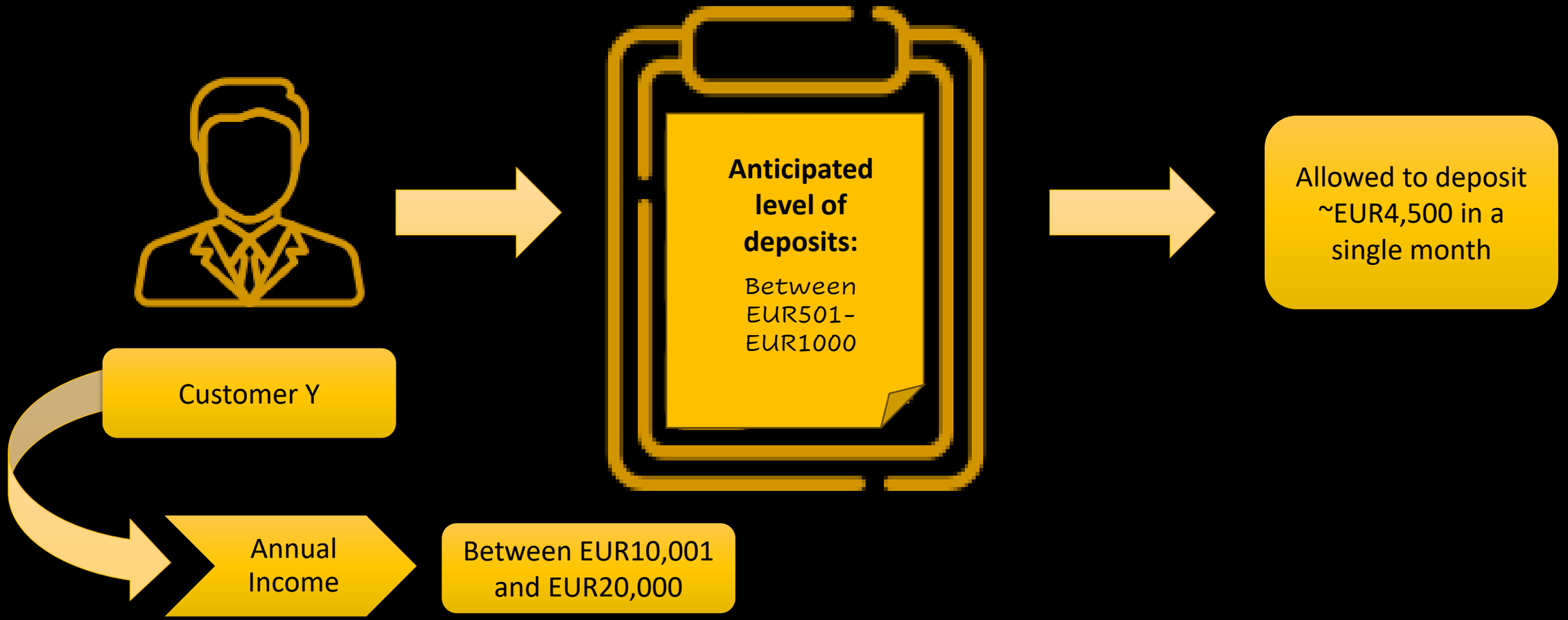
Large volume of transactions daily

Automated system



Issues with the Transaction Monitoring System – *Case Study cont.*

Further Issues relating to Transaction Monitoring – *Case Study*



Further Issues noted

Training

MLRO

Thank you!

Financial Intelligence Analysis Unit