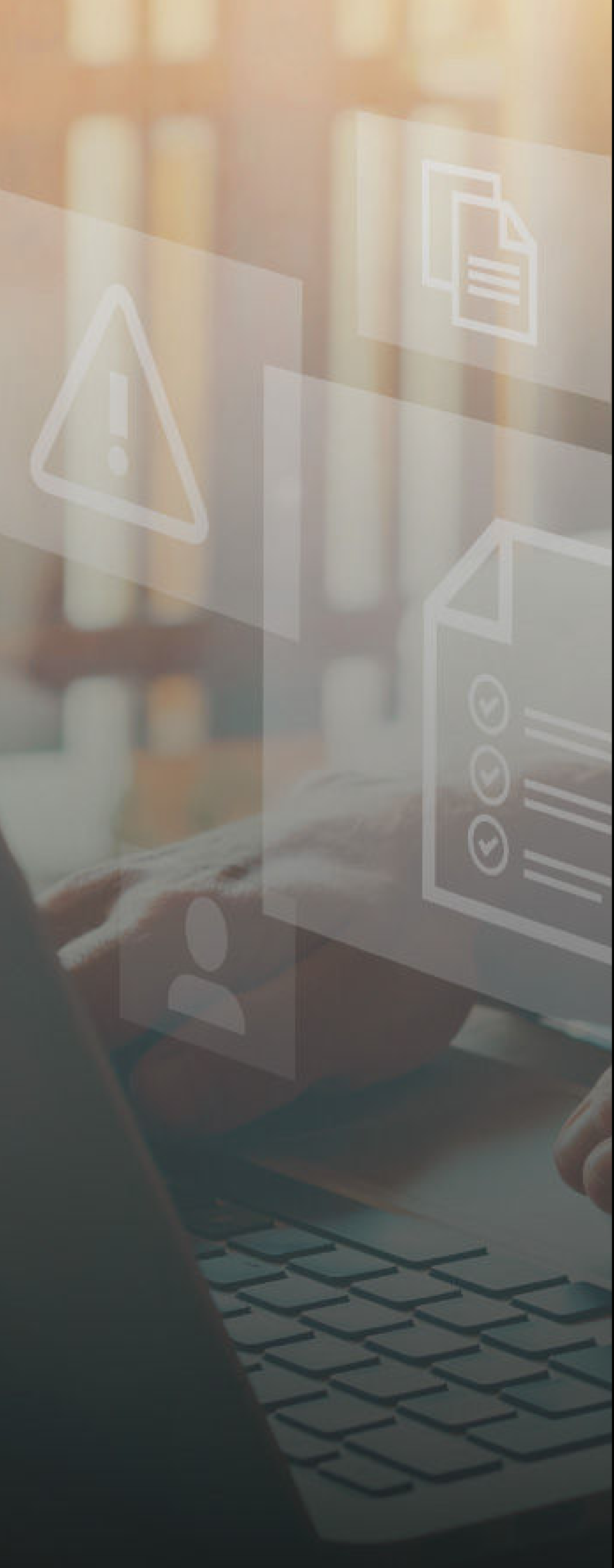
FIAU



goAML Rejection Rules

Published April 2024

Table of contents

Introduction

The purpose of this guidance document is to provide an overview of the Rejection Rules ensuing the Web Report validation process. These Rejection Rules serve as an added automated filter prior to the acceptance stage. This is to ensure that submissions made include as much information as possible to assist with the prompt assessment and prioritisation of reports being received by the FIAU.

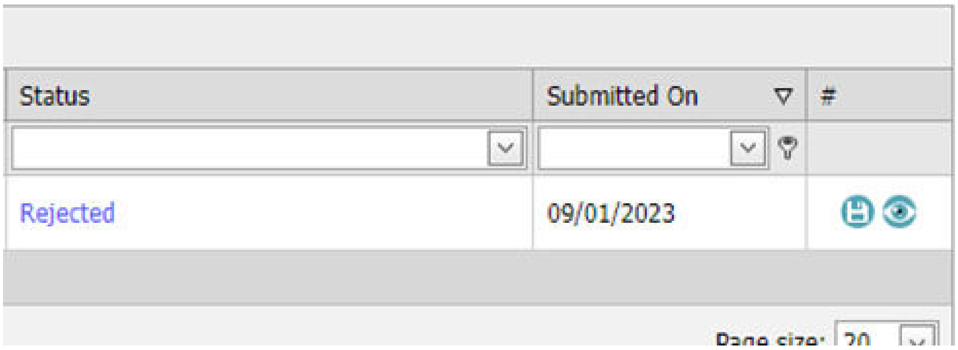
Some preliminary information in relation to Rejection Rules was already provided in the “Guidance Document on Reporting through goAML”, issued on 19th July 2022. This document goes into further details.

Validation of Reports

When submitting a report to the FIAU and the XML file is validated, the status changes to “Transferred from Web”. Following its approval based on XML validation and rejection rules by the FIAU’s screening officer, the status is changed to “Processed”. No action needs to be taken by reporting entities when the status of their submission is marked as “Processed”.

If the XML file submitted has any errors in the structure, then the status for the file can be seen as “Failed Validation”. This is only applicable for those reports uploaded directly via XML, as those submitted via a web report will always have a correct structure.

However, if there are mistakes or missing information in a validated XML file, then the screening officer may either manually or via GoAML rejection rules which are semi-automated reject the report by providing the reason for the rejection. A rejected report is marked as “Rejected” within the GoAML portal.



Status	Submitted On	#
Rejected	09/01/2023	

Page size: 20

Following the receipt of a “Failed Validation” or “Rejection”, reporting entities should correct the mistakes in the report and resubmit their submission. It is important to note that reports which are rejected, or which fail validation are not put through the analytical process, which means the report is not considered as having been submitted to the FIAU.

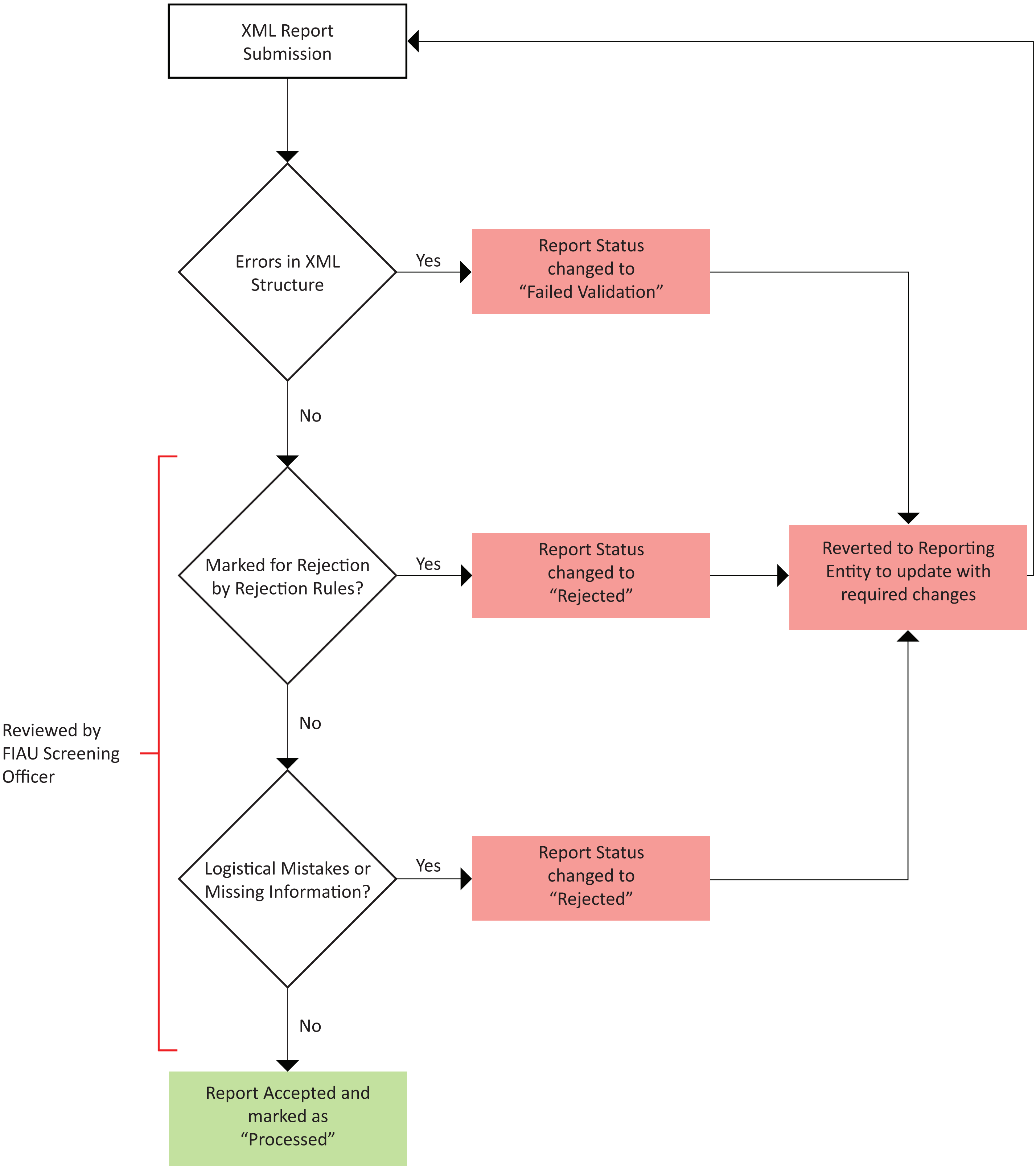

XML Report Submission
Errors in XML Structure
Yes
Report Status changed to "Failed Validation"
No
Marked for Rejection by Rejection Rules?
Yes
Report Status changed to "Rejected"
Reverted to Reporting Entity to update with required changes
No
Reviewed by FIAU Screening Officer
Logistical Mistakes or Missing Information?
Yes
Report Status changed to "Rejected"
No
Report Accepted and marked as "Processed"

Figure 1: XML Report Submission Flowchart

goAML Rejection Rules Validation

goAML rejection rules are automated validation checks which are conducted on new report submissions within goAML. These checks are based on a set of criteria to ensure a high level of data quality and analytical value, which is also used to feed into strategic analysis and risk assessments. Therefore, ensuring that the data being captured is structured and of good quality is of utmost importance.

When a report is marked for rejection by one of these rejection rules, the FIAU screening officer processing newly received reports is prompted with the reason for the validation errors. The screening officer manually confirms that these errors are present and if confirmed the report is rejected, and accompanied by a clear reason as to why it was rejected. Understanding why it was rejected is crucial for reporting entities, to not only amend and update their report but to help them avoid the same errors in future submissions. It is also imperative to highlight the fact that report rejections can may address more than one issue, at a time in a single rejected document, depending on the scenario, or circumstance.

Since the introduction of goAML, in June 2020, the FIAU has implemented 15 rejection rules within its goAML system. It is imperative to point out that data quality enhancements are crucial in the FIAU's line of work and as a result, these rejection rules may be enhanced or changed over time, depending on the needs of the Unit. This allows it to improve the quality and value of the data obtained at submission.

Most of the rejection rules implemented are related to checks on:

i) Report Indicators
ii) Transactions and Accounts
iii) Involved Entities and Persons
iv) Other – which relate to various aspects

This guidance document explains the above types of rejections rules to provide an understanding to reporting entities in terms of what is being expected by the FIAU with reference to report submissions.

Rejection Rules and Applicable Report Types

Report Type	STR	SAR	PEPR	PEPTR	TFR	TFTR	TRN	AIF
Rejection Rule								
R1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥
R2	🟥	🟥	🟩	🟩	🟩	🟩	🟥	🟥
R3	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥
R4	🟩	🟥	🟥	🟩	🟥	🟩	🟩	🟩
R5	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
R6	🟩	🟥	🟥	🟩	🟥	🟩	🟩	🟩
R7	🟩	🟥	🟥	🟩	🟥	🟩	🟩	🟩
R8	🟩	🟥	🟥	🟩	🟥	🟩	🟩	🟩
R9	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
R10	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
R11	🟥	🟩	🟩	🟥	🟩	🟥	🟥	🟥
R12	🟩	🟥	🟥	🟩	🟥	🟩	🟩	🟩
R13	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥
R14	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
R15	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥
R16	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥
R17	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩

Table 1: Rejection Rules across different reporting types

Rejection Rules – Report Indicators

R1 - Predicate Offence and Reason for Suspicion indicators for suspicious reports

At least one predicate offence should be selected within the report indicators. The option for ‘Unknown’ (Code: PO-2) should only be selected if the reporting entity has no indications of any possible predicate offence. If more than one predicate offence is suspected than multiple indicators can be selected. This is required by the FIAU to better understand the relevance and priority of the submitted report. Moreover, indicators such as the ones indicating the alleged predicate offence are very useful for statistical purposes, strategic analysis, guidance documents and risk assessments.

Code	Name
PO-1	Corruption and bribery (including kickbacks);
PO-10	Illicit trafficking in narcotic drugs and psychotropic substances
PO-11	Illicit trafficking in stolen and other goods
PO-12	Insider trading and market manipulation
PO-13	Kidnapping, illegal restraint and hostage-taking
PO-14	Murder, grievous bodily injury
PO-151	Organised crime - DOMESTIC- Participation in an organised criminal group and racketeering
PO-152	Organised crime - INTERNATIONAL - Participation in an organised criminal group and racketeering
PO-16	Piracy
PO-17	Revenues from organising illegal gambling
PO-18	Robbery or theft
PO-19	Traffic of Human Beings - Sexual exploitation
PO-191	Traffic of Human Beings - Sexual exploitation of children;
PO-2	Unknown - Predicate Offence could not be established
PO-20	Smuggling (including in relation to customs and excise duties and taxes)
PO-211	Tax Evasion - Corporate Income Tax
PO-212	Tax Evasion - Personal Income Tax
PO-213	Tax Evasion - Indirect Taxes: Stamp Duty, VAT, Import Duties, Excise Duty
PO-214	Tax Evasion - VAT Carousel

PO-215	Tax Crimes - Other
PO-22	Terrorism, including terrorist financing
PO-222	Targeted Financial Sanctions and Proliferation Financing (including dual-use goods)
PO-223	Proliferation Financing (including dual-use goods)
PO-231	Smuggling of Migrants
PO-232	Traffic of Human Beings - Forced Labour
PO-233	Traffic of Human Beings - Organ Removal
PO-24	Usury
PO-25	Counterfeiting Currency
PO-26	Illicit arms trafficking
PO-27	Prostitution and solicitation
PO-28	Cybercrime - Hacking/Unauthorized Access
PO-29	Cybercrime - Malware, Ransomware
PO-3	Counterfeiting currency
PO-30	Cybercrime - Phishing & other forms of social engineering
PO-31	Cybercrime - Other
PO-35	Embezzlement of funds
PO-36	Conducting a regulated activity without an adequate licence to do so (illegal gambling, underground banking, cheques, hawala etc.)
PO-37	Match-fixing
PO-4	Environmental crime
PO-5	Extortion
PO-6	Forgery
PO-711	Fraud - Identity Theft
PO-712	Fraud - Forged Documents
PO-713	Fraud - Debit and Credit Card
PO-714	Fraud - Cheque

PO-715	Fraud - Scams (non-delivery, sub par goods etc.)
PO-716	Fraud - Investment Scam
PO-717	Fraud - CEO/Business Email Compromise (BEC)
PO-718	Fraud - Other
PO-8	Fraud affecting the European Union financial interests
PO-9	Illegal gambling

Table 2: A list of all the Predicate Offences

The same concept applies for indicators relating to the Reason for Suspicion. If the reporting entity is not sure what to select one can choose ‘Other’ (Code: RS-12). Below is a list of the current indicators relating to the Reason for Suspicion.

Code	Name
RS-1	Unnecessarily Complex Structure - Ownership, Control
RS-10	Loans secured with assets held by third parties, unrelated to the borrower
RS-11	Name of the beneficiary and the name of the bank account to be credited do not match
RS-111	Unnecessarily Complex Series of Transactions
RS-12	Other
RS-13	Over or under-pricing of goods and services
RS-14	Purchasing camping/survival stores, first person shooting games or combat training-type activities, before travelling to know
RS-15	Proposed UBO/s changes after requesting identification details
RS-16	Life insurance policy: purchase without concern of the product's performance, paid in cash, or appears outside the customer's range of financial wealth
RS-17	Flight tickets purchasing to, or adjacent to, conflict zones or areas where terrorism activity is known to be present, without apparent family or business connections to those places
RS-18	Real estate is bought without viewing, with excessive urgency, lack of concern on expenses, or in the name of third parties
RS-19	Remitting money to locations which are in, or adjacent to, conflict zones or areas where terrorism activity is known to be present, without apparent family or business connections to those places
RS-2	Customer became uncooperative
RS-20	Remitting money to persons/entities (including NGOs) with suspected links to terrorism
RS-21	Safe deposit box visits are not in line with customer's profile (excessive)

RS-22	Selling off a significant part, or all, of one's personal assets, acquiring loans towards which insignificant or no payments are made, followed by travel and / or transactional activity to conflict zones or areas where terrorism ac
RS-23	Adverse Media - Subjects, or persons linked to subjects of STR are adversely known on open sources
RS-24	The anticipated source of payment of significant transactions (E.g. property or high value assets) is changed shortly before the purchase
RS-25	The majority of deposits and withdrawals are carried out through ATMs
RS-26	Transaction activity which is unexplained or is inconsistent with known customer profile
RS-27	Transaction narrative is suspicious or does not make any commercial sense within the context of the transaction itself
RS-28	Transfers to, or from, high-risk jurisdictions, without apparent economic business reason/sense
RS-29	Unusual or suspicious identification documents or lack of documents
RS-3	Customer inexplicably stops contact
RS-30	Withdrawal of money from locations which are in, or adjacent to, conflict zones or areas where terrorism activity is known to be present, without apparent family or business connections to those places
RS-31	Unusual denomination of bank notes used to effect deposits (e.g. EUR 1,000 in EUR 5 bank notes)
RS-32	Splitting of bets to remain below reporting threshold and thus avoiding CDD measures
RS-33	UBO disguise by involvement of third parties
RS-34	Funnelling/Channelling of funds
RS-35	Dark Web
RS-36	False documents
RS-37	Concealing Ownership
RS-38	Different IP address/Masking IP address
RS-39	Deposit, minimal gameplay and request for a withdrawal
RS-4	Payments to unrelated parties

RS-40	SoW/Sof - Unknown Sow/SoF (Source of Wealth/Source of Funds)
RS-41	SoW/Sof - Refusing to provide Sow/SoF information and/or documentation
RS-42	Withdrawals (large amounts, multiple etc.) conducted quickly after deposits
RS-43	Convictions
RS-44	Assets freeze
RS-45	Unexplained wealth: disproportionate assets, transactions and/or lifestyle compared to customer profile
RS-46	Indication of collusion via established link: same device, same IP, same card details, password etc.
RS-47	Usage of several/multiple debit/credit cards in the name of third-parties
RS-48	Legal person not filing required documents with authorities (e.g.: annual return, financial statements with MBR etc.)
RS-49	Trade-Based Money Laundering
RS-5	Excessive or accelerated repayments of long term loans (especially in cash)
RS-50	RS-49
RS-51	Chip Dumping
RS-6	High turnover, low balance being kept (E.g. conduit account activity)
RS-7	High value asset is sold shortly after being purchased
RS-8	High value purchases paid in cash
RS-9	Large volume of deposits, not in line with customer's known profile

Table 3: Reason for Suspicion Indicators Table

R2 - Report Specific Indicators (TF/PEPs)

Reporting entities should include report specific indicators for specific report types, namely for Terrorist Financing (TF) or Politically Exposed Persons (PEPs) related reports.

Report Type	Indicators
TFR/ TFTR	PO-22 - Terrorism, including terrorist financing
PEPR/ PEPTR	RT-215 – Current PEP EU: Involvement of an EU PEP in the situation reported; OR RT-213 - Current PEP International (non-EU): Involvement of an international PEP in the situation reported; OR RT-211 - Current PEP National: Involvement of a national PEP in the situation reported; OR RT-216 - Former PEP EU: Involvement of a former EU PEP in the situation reported; OR RT-214 - Former PEP International (non-EU): Involvement of a former international PEP in the situation reported; OR RT-212 - Former PEP National: Involvement of a former national PEP in the situation reported;

Table 4: A list of all the Predicate Offences and related report indicators

R3- Call for Action: High-Risk Jurisdictions

Subject persons are required to include “Call for Action: High-Risk Jurisdictions subject to a Call for Action” (Code: RT-33) as a report indicator, if the involved person being reported is linked with a high-risk jurisdiction, such as Iran and a report is being submitted via goAML in line with Regulation 15(4). This indicator once again is essential for the FIAU to flag and prioritise such reports, accordingly. Especially, because the FIAU is obliged to reply to the reporting entity within a five-day period.

To this effect, the FIAU had issued a specific notice in addition to a guidance note in relation to the reporting of such transactions connected to High-Risk Jurisdictions, please refer to:

- https://fiaumalta.org/news/fatf-jurisdictions-important-notice-with-respect-to-iran/
- https://fiaumalta.org/wp-content/uploads/2022/07/1792-FIAU-Guidance-Document-goAML.pdf

Rejection Rules and Applicable Report Types

R4 - Reports with Multiparty Transactions

Transactions within reports should always be bi-party transactions. Multi-party transactions will not be processed and accepted by the FIAU. This approach was adopted by the FIAU to simplify as much as possible transactions and thus be able to analyse the activity via GoAML in a more uniform manner.

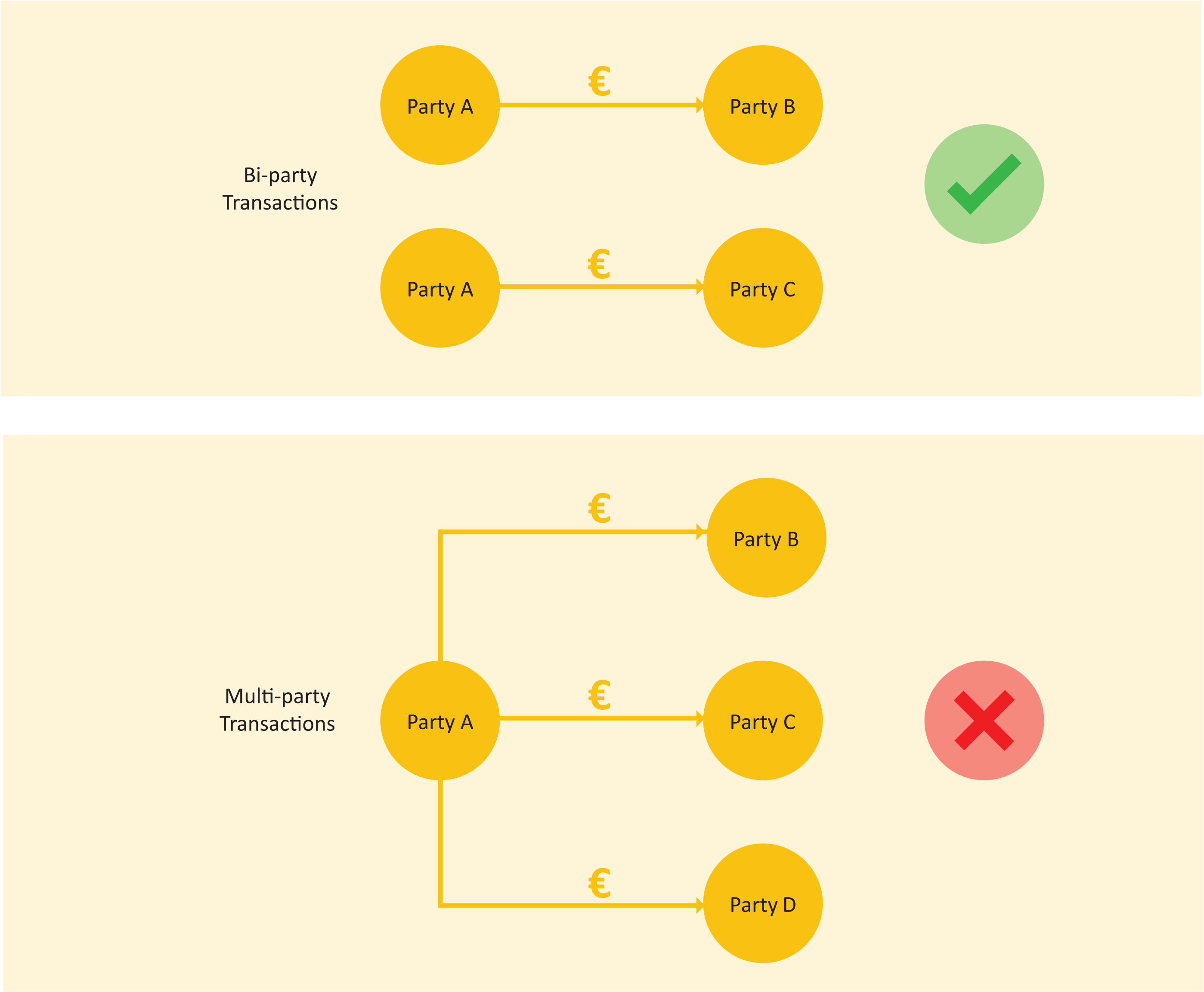
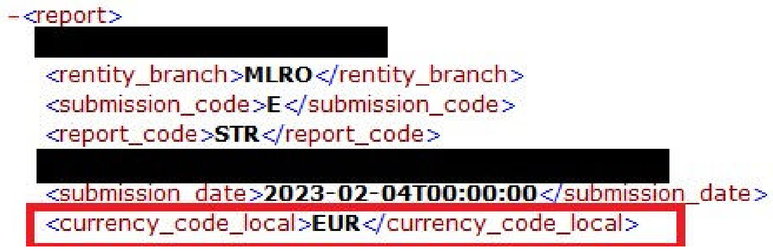


Figure 2: BI-Party versus Multi-Party Transactions

R5 - Local Currency Code

The ‘currency_code_local’ should always be set to ‘EUR’ when submitting reports via XML. If it is provided as another currency via XML the report will automatically be marked for rejection. Essentially, as an FIU our main currency on goAML is set as ‘EUR’, however, the system itself provides reporting entities the ability to include exchange rates accordingly. The foreign currency code is used when a transaction, is carried out in a currency other than ‘EUR’, to have full visibility of the exchange rate. In this case, the Reporting Entity must report the transaction with its actual details including the use of foreign currency along with the rate of conversion used on that day.

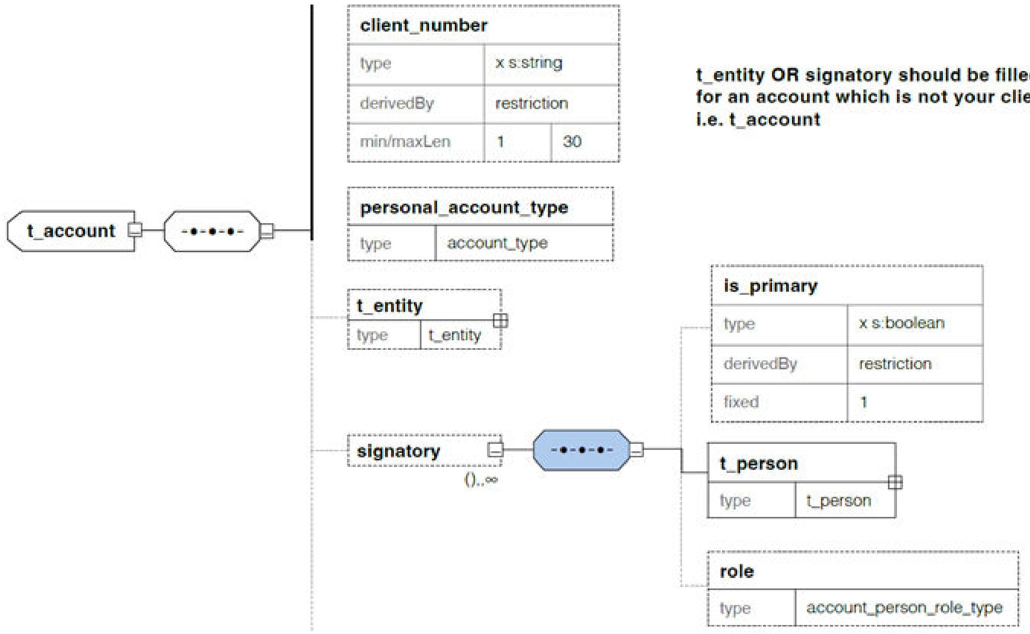


```
- <report>
   [redacted]
   <rentity_branch>MLRO</rentity_branch>
   <submission_code>E</submission_code>
   <report_code>STR</report_code>
   [redacted]
   <submission_date>2023-02-04T00:00:00</submission_date>
   <currency_code_local>EUR</currency_code_local>
```

R6 - Transactions which have no account holders

Third party accounts (non-clients of the reporting entity) listed within submissions should be accompanied with at least one entity (t_entity) or one signatory. The names provided should reflect the account holder name associated with the respective account. The FIAU understands that the data provided is limited to what the subject person has available and thus cannot be confirmed by the reporting entity. Nevertheless, it is still important that the added nodes and data are provided to the FIAU for processing and added analytical purposes.

In turn, where client accounts are included in reporting submissions, reporting entities must always provide all signatories and entities (if applicable) associated with the account.



t_entity OR signatory should be filled in for an account which is not your client i.e. t_account

Figure 3: Entities and signatory nodes associated with Accounts

R7 - Transactions which are post dated

Transaction dates (‘date_transaction’ field) should not be post-dated within reports. While a number of payments can be post-dated in a number of different circumstances, these are not permissible upon submission.

R8 - Transaction with no value (zero as amount)

It is imperative to highlight that to have good quality data, subject persons should ensure that the transaction value (‘amount_local’ field) should never have a value of zero.

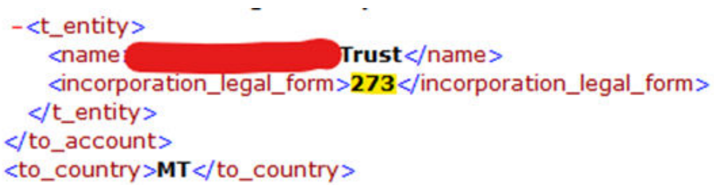
R9 - Updating of closing date when an account is closed or blocked

Reporting entities are required to provide the closing date of an account (‘closed’ field within the account node) when the status is marked as ‘Closed’ (goAML code: ‘CL’) or ‘Blocked’ (goAML code: ‘BL’). From an analytical perspective, it’s a crucial piece of information, thus extremely important to be filled in.

Rejection Rules – Involved Entities and Persons

R10 - Trusts should be marked as ‘Trust’ within the legal form

Any designated trusts should be adequately indicated accordingly within the involved entities immediately upon report submission. Predominantly, it should be marked as ‘Trust’ (Code: 273) within the legal form (‘incorporation_legal_form’).



```
-<t_entity>
   <name[redacted]Trust</name>
   <incorporation_legal_form>273</incorporation_legal_form>
 </t_entity>
</to_account>
<to_country>MT</to_country>
```

Figure 4: Proper Trust designation via XML

R11 - Involved Persons - Date of Birth (Activity Reports)

One of the most critical and crucial elements of intelligence analysis are basic identifiable details such as the date of birth. It is very important that the date of birth for involved persons within activity reports is not left blank or filled in with erroneous data such as ‘01/01/1900’. This is fundamental for data quality purposes and to have a form of identification with the full name of the involved person within the report.

R12 - Involved Persons - Date of Birth (Transactional Reports)

Date of birth for involved persons within transactional reports who are clients of the reporting entity should not be left blank or filled in with erroneous data such as ‘01/01/1900’. This is fundamental for data quality purposes and to have a form of identification with the full name of the involved person within the report.

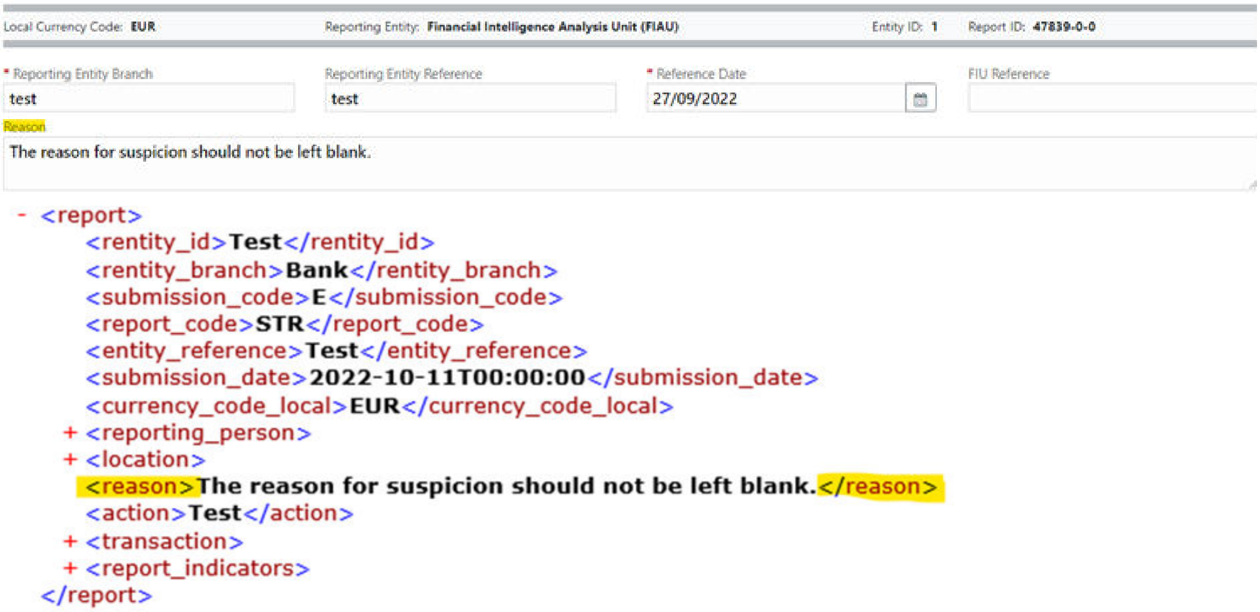
R13 - Involved Persons - Nationality

Nationality for involved persons who are clients of the reporting entity should be provided and not marked as ‘UNKNOWN’. This rejection rule is not applicable for the remote gaming industry because the minimum level of customer due diligence required does not entail collecting such details. The nationality is mostly vital as it enables the FIAU to identify new links with foreign jurisdictions.

Rejection Rules – Other

R14 - Reason for suspicion

The reason for suspicion ('reason' field) needs to be filled for all report types except for the Additional Information Files (AIFs). A summary of the suspicion should be provided within this field, while a full detailed report can be provided as an attachment to the report. However, it is very important to include a summary within this field.



Local Currency Code: **EUR**	Reporting Entity: **Financial Intelligence Analysis Unit (FIAU)**	Entity ID: **1**	Report ID: **47839-0-0**
* Reporting Entity Branch	Reporting Entity Reference	* Reference Date	FIU Reference
test	test	27/09/2022	

Reason

The reason for suspicion should not be left blank.

```
- <report>
      <rentity_id>Test</rentity_id>
      <rentity_branch>Bank</rentity_branch>
      <submission_code>E</submission_code>
      <report_code>STR</report_code>
      <entity_reference>Test</entity_reference>
      <submission_date>2022-10-11T00:00:00</submission_date>
      <currency_code_local>EUR</currency_code_local>
    + <reporting_person>
    + <location>
      <reason>The reason for suspicion should not be left blank.</reason>
      <action>Test</action>
    + <transaction>
    + <report_indicators>
  </report>
```

R15 – Reporting Entity Reference

The reporting entity reference ('entity_reference') should be included within any report submitted to the FIAU. This reference refers to an internal reference used by the reporting entities submitting the report. This is required to facilitate communication between the FIAU and the reporting entity.

R16 - Attachments Required

It is expected that a report submission is backed by supporting documentation. This is a requirement to ensure that the FIAU is privy to the same information available to the subject person. Thus, enabling it to reach the same conclusions based on the same facts as the subject person submitting the report.

R17 – FIU Ref No. Required when submitting AIF and TRN reports

When submitting TRN and AIF reports it is required to provide the report key also known as the 'report submission reference' of the previously submitted report (such as an STR) within the 'fiu_ref_number' field. The 'report submission reference' is usually in this format ('12345-0-0') and is provided both in the GOAML portal 'Submitted Reports' section and in a notification sent via the 'Message Board' once the report is submitted.

Conclusion

In the case of any additional queries in terms of transactional activity reporting or XML Schema submissions, kindly refer to the Technical Documentation on the FIAUs website (Refer: https://fiaumalta.org/report-a-suspicion) otherwise kindly forward an email to the below mentioned email addresses.

- goAMLsupport@fiaumalta.org
- goAMLtechnical@fiaumalta.org

D F G H
X C V B N M
⌘
command
hly Report of Financial Situation
5th 6th 7th 8th 9th 10th 11th 12th

Questions on this document may be sent to
goAMLsupport@fiaumalta.org or goAMLtechnical@fiaumalta.org

Financial Intelligence Analysis Unit
Trident Park, No. 5, Triq l-Mdina,
Central Business District
Birkirkara, CBD 2010

Telephone: (+356) 21 231 333
Fax: (+356) 21 231 090
E-mail: info@fiaumalta.org
Website: www.fiaumalta.org