USER GUIDE TO SUBMIT SUSPICIOUS ACTIVITY REPORTS (SAR) ON THE REGISTRATION AND REPORTING PLATFORM OF THE FINANCIAL INTELLIGENCE CENTRE VERSION 3.0
Legal Disclaimer

Unless specific written consent is obtained from the Financial Intelligence Centre, the information contained in this document may not be shared with any third parties.

By reading this document, you acknowledge the confidentiality of such and agree to be bound by the copyright that subsists in Financial Intelligence Centre’s intellectual ideas, views and their representation as expressed in this material.
Objective of this guideline

The objective of this user guide is to define and outline the steps to be followed when submitting a Suspicious Activity Report (SAR) to the Financial Intelligence Centre (the FIC) in terms of section 29 of the FIC Act. Please note that the reporter must acquire login credentials on the FIC’s registration and reporting platform, goAML, in order to access the reporting platform. Please refer to Public Compliance Communication 05B for guidance on registration with the FIC and acquisition of login credentials on the registration and reporting platform.

This user guide is applicable to a person who carries on a business or is in charge of or manages a business or is employed by a business and includes all accountable institutions listed in Schedule 1 to the FIC Act and all reporting institutions listed in Schedule 3 to the FIC Act.

This user guide is not issued in terms of section 4(c) of the FIC Act and is therefore not formal guidance issued by the FIC.

Access to the registration platform

In order to submit an SAR to the FIC, the accountable institution or reporting institution or any other person who is to report to the FIC, must access the portal provided by the FIC for this purpose on the FIC’s website at www.fic.gov.za

Legal Disclaimer

The FIC reserves the right to amend, modify or change the contents of this document.
Glossary

This guideline must be read in conjunction with the FIC Act and the Money Laundering and Terrorist Financing Control Regulations made in terms of section 77 of the FIC Act. In this guideline, unless the context indicates otherwise:

“Al/RI” refers to an accountable institution (listed in Schedule 1 to the FIC Act) and reporting institution (listed in Schedule 3 to the FIC Act).

“Business” refers to organisation, institution or entity (ies) and can be used interchangeably.

“Compliance Officer” refers to a person who is tasked, for purposes of the registration and reporting process, to ensure that the details of the accountable institutions are correctly submitted and maintained on the FIC’s website, and regulatory reports are submitted successfully.

“FIC Act” refers to the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001).

“goAML” refers to an integrated software solution implemented by the FIC as its preferred IT platform for registration, reporting, data collection, analysis, case management and secure communications required for the FIC’s daily operational functions and requirements.

“Money laundering reporting officer” (MLRO) is envisaged to be a person, other than the Compliance Officer, with the responsibility and authority to submit regulatory reports to the FIC on behalf of the accountable or reporting institution. Not all Al/RI’s will have MLRO’s. Institutions that require reports to be submitted by persons other than the Compliance Officer, must register an MLRO. The MLRO will have his/her own login credentials, he/she may not use the Compliance Officer’s credentials to fulfil this role. On goAML there will be various MLRO roles.
**MLRO roles are:**

- MLRO Web Reporting (Money Laundering Reporting Officer - applicable to web reporting only)
- MLRO Batch Reporting (Money Laundering Reporting Officer - applicable to batch reporting only)
- MLRO All (Money Laundering Reporting Officer - all reporting and message board).

“**Person**” refers to a natural person who registers to file a report in terms of section 29 of the FIC Act in their own personal capacity or **MLRO** as defined.

“**Regulations**” refer to the Money Laundering and Terrorist Financing Control Regulations made in terms of section 77 of the FIC Act and promulgated in Government Notice 41154 of 29 September 2017 as amended.

“**Reporting entity**” refers to an accountable institution, reporting institution or any other person or institution, that is submitting a report to the FIC.

“**SAR**” refers to a suspicious or unusual activity report submitted in terms of section 29 of the FIC Act.

“**Targeted Financial Sanctions (TFS)**” refers to the measures to restrict sanctioned persons and entities from having access to funds and property under their control and from receiving financial services in relation to such funds and property by requiring accountable institutions, reporting institutions and other persons to freeze property and transactions pursuant to financial sanctions imposed in the United Nations Security Council (UNSC) Resolutions.

**Important information to remember when reporting on the FIC’s reporting platform:**

- Accountable and reporting institutions must register in terms of the FIC Act before a SAR can be submitted. Please refer to registration guideline for accountable and reporting institutions and PCC 05B for registration related information.
- All fields with an asterisk (*) are mandatory and should be completed.
• The user needs to consider business rules applicable to the various regulatory reports when reporting and apply them along with the applicable regulations and sections of the FIC Act.

• All fields on the regulatory report should be completed with full particulars of information that the institution is expected to have as either part of the course of establishing a particular person’s identity or the conducting of a particular transaction(s).

• All fields on the regulatory report, that are not obtained during the course of establishing a particular person’s identity or conducting a particular transaction, but should be obtained as part of commercial practice, should be completed with as much of the information as readily available. In an instance where the reporting institution does not have information readily available, they are to populate mandatory fields with “not obtained”.

• We advise all users to clear/delete their browsing histories frequently and restart their browsers afterwards. This should include the deletion of cookies and passwords in order for the new goAML web forms to load correctly.

• All First Letters of words must be in Capital Letters.

• Words typed in ALL Capital Letters are not allowed.

• The FIC does not accept any regulatory reports submitted unless it was submitted on the goAML system. Regulatory reports must accordingly be submitted in the prescribed format and timeframes. Failure to submit regulatory reports within the prescribed timeframes constitutes a finding of non-compliance in terms of the FIC Act. Always report any goAML incidents/queries to the FIC immediately.

• Ensure that all users log relevant ICT queries / incidents to the FIC by means of the formal channels.
1. Table of Contents

1. Table of Contents .................................................................................................................. 7
2. Introduction ........................................................................................................................... 9
3. goAML Web Icons ................................................................................................................ 10
4. Suspicious Activity Report (SAR) Baseline Scenario ........................................................... 11
4.1 Field Definitions .................................................................................................................. 11
4.2 Baseline scenario for submitting a suspicious activity report (SAR) to the FIC where the person is NOT the client of the AI/RI – displaying fields A to G to be completed .................. 13
4.3 Baseline scenario for submitting a single suspicious activity report to the Centre where the person is the client of the AI/RI – displaying fields A to G to be completed .................................. 14
4.4 Baseline scenario for submitting a single suspicious activity report to the Centre where the person is the client of the AI/RI and has attempted to transact— displaying fields A to G to be completed .................................................................................................................. 15
4.5 Baseline scenario for submitting a single suspicious activity report to the Centre WITH goods or services – displaying fields A to G to be completed ......................................... 16
4.6 Baseline scenario for submitting a suspicious activity report to the FIC related to Targeted Financial Sanctions – displaying fields A to H to be completed ......................................... 17
5. Accessing goAML .................................................................................................................. 18
6. goAML platform landing page ............................................................................................ 19
7. Capturing a Suspicious Activity Report ............................................................................ 20
7.1 Select a new Report ............................................................................................................ 20
7.2 Reporting template - overview ......................................................................................... 20
BASELINE SCENARIO FIELD A – REPORT TYPE .................................................................. 21
7.3 Select Report Type ............................................................................................................ 21
BASELINE SCENARIO FIELD B – REPORTING PERSON AND LOCATION .............................. 23
7.4 Reporting Person .............................................................................................................. 23
7.5 Location ........................................................................................................................... 23
7.6 Editing the Location ......................................................................................................... 23
BASELINE SCENARIO FIELD C – INDICATORS .................................................................. 24
7.7 Indicators .......................................................................................................................... 24
BASELINE SCENARIO FIELD D – ACTIVITY ....................................................................... 26
7.8 Activity .............................................................................................................................. 26
BASELINE SCENARIO FIELD E – REPORTING PARTIES ..................................................... 28
7.9 Reporting parties .............................................................................................................. 28
BASELINE SCENARIO FIELD F – PARTY TYPE (PERSON / ACCOUNT / ENTITY) ................ 29
7.10 Party Type ....................................................................................................................... 29
7.11 Person Form ..................................................................................................................... 29
7.12 Phone .............................................................................................................................. 32
7.13 Address .......................................................................................................................... 32
7.14 Identification .................................................................................................................. 33
7.15 Email ............................................................................................................................... 33
7.16 Employer Address and Employer PhoneClicking the Employer Address / Phone add button generates person’s employers form to be completed ......................................................... 33
7.17 Save and Cancel Button ................................................................................................. 33
7.18 Account ........................................................................................................................... 34
7.19 Entity ............................................................................................................................... 37
BASELINE SCENARIO FIELD G – GOODS AND SERVICES ................................................ 40
7.20 Goods and Services ........................................................................................................ 40
7.21 Adding Multiple Parties to Activity Report ...................................................................... 41
7.22 Saving / Submitting the report ....................................................................................... 42
8. Reviewing saved and submitted reports ............................................................................. 45
8.1 Reviewing a saved report ................................................................................................ 45

User guide to submit suspicious activity reports (SAR) on the registration and reporting platform of the Financial Intelligence Centre

Version 3.0 | 21 August 2019
8.2 Reviewing a submitted report

8.2 Reviewing report status via the Message Board

9. Important reporting tips

10. Reporting Process workflow
2. Introduction

A person who carries on a business or is in charge of or manages a business or is employed by a business, including all accountable institutions listed in Schedule 1 to the FIC Act and all reporting institutions listed in Schedule 3 to the FIC Act have an obligation to submit suspicious or unusual activity reports (SAR) to the FIC in terms of section 29 of the FIC Act and must utilise the FIC’s registration and reporting platform, goAML, for submitting SAR to the FIC. It is important to note that section 29 of the FIC Act refers to reports of suspicious or unusual activity concerning the proceeds of unlawful activities, money laundering, terrorist financing and financial sanctions offences as opposed to criminal activity in general. A SAR must be submitted in respect of when a suspicion relates to the proceeds of unlawful activity, or money laundering activity or a contravention of prohibitions under S26B of the FIC Act.

goAML is accessible on the FIC’s website, www.fic.gov.za, and selecting the “Register or Report” functionality.
### 3. goAML Web Icons

<table>
<thead>
<tr>
<th>Icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="add.png" alt="Add Icon" /></td>
<td>Add</td>
</tr>
<tr>
<td><img src="cancel.png" alt="Cancel Icon" /></td>
<td>Cancel instructs goAML not to capture the detail</td>
</tr>
<tr>
<td><img src="close.png" alt="Close Icon" /></td>
<td>Close</td>
</tr>
<tr>
<td><img src="preview.png" alt="Preview Icon" /></td>
<td>Preview</td>
</tr>
<tr>
<td><img src="print.png" alt="Print Icon" /></td>
<td>Print</td>
</tr>
<tr>
<td><img src="remove.png" alt="Remove Icon" /></td>
<td>Remove the uploaded document</td>
</tr>
<tr>
<td><img src="upload.png" alt="Upload Icon" /></td>
<td>Upload a document</td>
</tr>
<tr>
<td><img src="save.png" alt="Save Icon" /></td>
<td>Save</td>
</tr>
<tr>
<td><img src="save-report.png" alt="Save Report Icon" /></td>
<td>Save a report</td>
</tr>
<tr>
<td><img src="submit-report.png" alt="Submit Report Icon" /></td>
<td>Submit a report</td>
</tr>
<tr>
<td><img src="show-attachments.png" alt="Show Attachments Icon" /></td>
<td>Shows the number of attached documents</td>
</tr>
<tr>
<td><img src="new-reports.png" alt="NEW REPORTS Icon" /></td>
<td>Upload XML and web reports</td>
</tr>
<tr>
<td><img src="drafted-reports.png" alt="DRAFTED REPORTS Icon" /></td>
<td>Access drafted and submitted reports</td>
</tr>
<tr>
<td><img src="submitted-reports.png" alt="SUBMITTED REPORTS Icon" /></td>
<td>View submitted reports</td>
</tr>
<tr>
<td><img src="message-board.png" alt="MESSAGE BOARD Icon" /></td>
<td>Access mail messages on goAML</td>
</tr>
<tr>
<td><img src="my-goaml.png" alt="MY GOAML Icon" /></td>
<td>Change password and user details</td>
</tr>
<tr>
<td><img src="admin.png" alt="ADMIN Icon" /></td>
<td>Access statistics</td>
</tr>
<tr>
<td><img src="logout.png" alt="LOGOUT Icon" /></td>
<td>Logout of goAML</td>
</tr>
</tbody>
</table>
4. Suspicious Activity Report (SAR) Baseline Scenario

The below process flow diagram demonstrates the end-to-end process of uploading a SAR. This diagram is given greater detail in the content below. Fields in the flow diagram are labelled A to H.

4.1 Field Definitions

- Report type (A) – The type of report (i.e. SAR)
- Reporting Person and Location (B)
  - Reporting Person - Linked to the logged in user details, this is the person uploading the SAR
  - Location - Describes the actual geographical area / branch where the proposed, cancelled or attempted transaction or series of transaction or suspicious and unusual activity occurred. The address of the logged in user is populated in the selected report for capturing. The logged in user must edit or delete the address, if the populated address is not the actual location of where the transaction (series of transactions) and/or unusual/suspicious activity occurred
- Indicators (C) – Indicators are used to specify the nature or type of suspicious or unusual activity that the institution is reporting to the FIC. The institution is required to review the list of pre-determined indicators and select the most appropriate explanation(s).
- Activity (D) - Activity – can refer to an abandoned, proposed, cancelled or attempted transaction, as well as any other non transaction based activity. An activity is based on suspicion.
- Report parties (E) and Person / Entity / Account (F)
  - Person - this refers to a natural person
    Note: If a person physically receives or pays cash, “person” is selected
  - Entity - this refers to a legal person. Note that there is a natural person that will always be linked to an entity (i.e. The signatory)
Note: If an entity physically receives or pays cash, “entity” is selected

- Account - this refers to an account held with an accountable institution (e.g. Cheque account held with a bank)

  Note: When cash is deposited or withdrawn to/from an account, then “account” will be selected

- Mandatory Fields (G) – this refers to the fields that are compulsory to be completed. The information that is required is dependent on the fields selected in field G (i.e. Person / Entity / Account)

- Goods and services – this information is required to further describe the physical assets that are linked to the report submitted. This is only compulsory should this be a physical asset (i.e. Where there is more to the transaction than just the flow of funds), and is captured as the last step of the report capturing prior to ‘saving and submitting’ to the FIC. The following information is mandatory when completing this section:

  - Item type – if this is a moveable or immovable property within or outside the Republic of South Africa
  - Description – brief description of the property involved (e.g. Luxury vehicle)
  - Address – address where the property can be located
  - Estimated value - estimated value of the property at time of report being submitted
### 4.2 Baseline scenario for submitting a suspicious activity report (SAR) to the FIC where the person is NOT the client of the AI/RI – displaying fields A to G to be completed

#### Suspicious and Unusual Activity Report (SAR) - Baseline Scenario

<table>
<thead>
<tr>
<th>Example</th>
<th>A Report Type</th>
<th>B Reporting Person, Location</th>
<th>C Indicators</th>
<th>D Activity</th>
<th>E Report Parties</th>
<th>F Person / Account Number / Entity / Transaction Item</th>
<th>G Mandatory fields: *</th>
</tr>
</thead>
</table>
| Mr X attempts to deposit funds of R50 000 at Attorney C. Mr X refuses to comply with KYC requirements. | **Suspected and Unusual Activity Report (SAR)** Reason for Report: *Mr X refuses to comply with KYC requirements as required in terms of the FIC Act.* Action (free text): Let relevant actions as per internal risk framework for example: SAR referred to FIC. *Internal flagging as per internal policy* | **Attorney C** Reporting Person and Location of report information **Reported information will be processed automatically** | **Select one or more applicable indicators** | **4a. Report Parties** | **Person** | **4b. Goods and Services** ONLY for physical assets | **Person**  
*Full name*  
*Surname*  
**Account Number**  
*Account number*  
*Institution name*  
**Entity**  
*Name*  
**Transaction Item**  
*Item Type*  
*Description*  
*Estimated Value* |
4.3 Baseline scenario for submitting a single suspicious activity report to the Centre where the person is the client of the AI/RI – displaying fields A to G to be completed

<table>
<thead>
<tr>
<th>Example</th>
<th>A: Report Type</th>
<th>B: Reporting Person, Location</th>
<th>C: Indicators</th>
<th>D: Activity</th>
<th>E: Report Parties</th>
<th>Person / Account Number / Entity / Transaction Item</th>
<th>F: Mandatory fields</th>
</tr>
</thead>
</table>

- **Person**
  - Title
  - Gender
  - Full name
  - Surname
  - Date of birth
  - ID number
  - Nationality
  - Residence
  - Non-RSA ID / Passport
  - Issuing country
  - RSA Passport
  - Address
  - Telephone number

- **Account Number**
  - Account number
  - Institution name
  - Branch
  - Financial institution
  - Institution code or Swift code
  - Account type
  - Status
  - Currency code
  - Date opened
  - Balance
  - Date of balance
  - Entity
  - Signatory

- **Entity**
  - Name
  - Registered name
  - Incorporated legal form
  - Incorporation registration number
  - Incorporation country
  - Telephone number
  - Address
  - Director (one or more)

- **Transaction Item**
  - Item Type
  - Description
  - Estimated Value
  - Address

**Suspicious and Unusual Activity Report (SAR) - Client refuses to provide information about source of funds**

- **Log in:** Bank Y
- **1. Report Type**
  - Client Mr X of Bank Y attempts to deposit a cash amount of R45 000 at Branch Z. After enquiring about the source of funds, Mr X decides not to deposit the cash.

- **2. Reporting Person, Location**
  - Suspicious and Unusual Activity Report (SAR)
  - Reason for Reporting: Mr X
  - Attempted transaction connection by the X when enquiries was made about the source of funds
  - Action (if any)
  - List relevant actions as per internal risk framework
  - Example: *SAR reported to FIC*

- **3. Indicators**
  - Reporting Person Info
  - Location of report
  - Reports information fields automatically

- **4a. Report Parties**
  - *Person
  - *Account Number

- **4b. Goods and Services**
  - *Transaction Item
  - *Description
  - *Estimated Value

- **Address**
4.4 Baseline scenario for submitting a single suspicious activity report to the Centre where the person is the client of the AI/RI and has attempted to transact—displaying fields A to G to be completed

<table>
<thead>
<tr>
<th>Example</th>
<th>Report Type</th>
<th>Reporting Person, Location</th>
<th>Indicators</th>
<th>Activity</th>
<th>Report Parties</th>
<th>Person / Account Number / Entity / Transaction Item</th>
<th>Mandatory fields:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Advisor B’s Client Company X makes an enquiry to structure prospective payments in an attempt to conceal the underlying client and ultimate beneficiary.</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log in: Financial Advisor B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Report Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Susicious and Unusual Activity Report (SAR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reason for Reporting (SAR): Client Company X makes an enquiry to structure prospective payments in an attempt to conceal the underlying client and ultimate beneficiary.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action field</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List relevant actions as per internal risk framework for example: “SAR reported to PIC” “Internal flagging as per internal Policy”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting Person, Location</td>
<td>Indicators</td>
<td>Activity</td>
<td>Report Parties</td>
<td>Person / Account Number / Entity / Transaction Item</td>
<td>Mandatory fields:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.4 Baseline scenario for submitting a single suspicious activity report to the Centre where the person is the client of the AI/RI and has attempted to transact—displaying fields A to G to be completed
4.5 Baseline scenario for submitting a single suspicious activity report to the Centre WITH goods or services – displaying fields A to G to be completed

<table>
<thead>
<tr>
<th>Example</th>
<th>A Report Type</th>
<th>B Reporting Person, Location</th>
<th>C Indicators</th>
<th>D Activity</th>
<th>E Report Parties</th>
<th>F Person / Account Number / Entity / Transaction Item</th>
<th>G Mandatory fields:*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mr Q makes enquiries with Estate Agent X to purchase a property and register it in a relative’s name in order to hide his assets from the revenue service.</td>
<td>Log in: Estate Agent X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Report Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Suspicious and Unusual Activity Report (SAR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reason for Reporting (free text)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Client Mr Q makes an enquiry to register a property in the name of a relative in order to conceal the asset from the revenue service and may be involved in tax evasion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action (free text)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>List relevant actions as per internal risk framework for example: *SAR reported to FIC *Internal logging as per internal policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Estate Agent X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reporting Person and Location of report information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>**Relevant information pulled through automatically</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Indicators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select one or more applicable indicators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4a. Report Parties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4b. Goods and Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>*Person</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>*Account Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>*Entity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>*Transaction Item</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Item Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>House Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Estimated Value</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R1,5 million</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User guide to submit suspicious activity reports (SAR) on the registration and reporting platform of the Financial Intelligence Centre

Version 3.0 | 21 August 2019
4.6 Baseline scenario for submitting a suspicious activity report to the FIC related to Targeted Financial Sanctions – displaying fields A to H to be completed

Baseline Scenario – Suspicious Activity Report (SAR) – Reporting a suspicious and unusual activity involving targeted financial sanctions (TFS)

- **Person**
  - Name
  - Gender
  - Full name
  - Surname
  - Date of birth
  - ID number
  - Nationality
  - Residency
  - Non-RSA ID / Passport
  - Issuing country
  - RSA Passport
  - Address
  - Telephone number

- **Account Number**
  - Account number
  - Institution name
  - Branch
  - Financial Institution
  - Institution code or SWIFT code
  - Account type
  - Status
  - Currency code
  - Date opened
  - Balance
  - Date of balance
  - Entity
  - Signatory

- **Entity**
  - Name
  - Registered name
  - Incorporated legal form
  - Incorporation / Registration number
  - Incorporation country
  - Telephone number
  - Address
  - Director (one or more)

- **Transaction Item**
  - Item Type
  - Description
  - Address
  - Estimated Value

---

User guide to submit suspicious activity reports (SAR) on the registration and reporting platform of the Financial Intelligence Centre

Version 3.0 | 21 August 2019

Page 17 of 53
5. Accessing goAML

Accountable and reporting institutions can access the goAML platform by utilising the username and password captured during the registration process. Authentication will always be required before gaining access to goAML.

- Go to the FIC’s website, www.fic.gov.za and select the “Click here to REGISTER OR REPORT” banner
- Access goAML page by clicking on reporting forms; OR access the link directly by using https://goweb.fic.gov.za/goAMLWeb_PRD
- Click on the Login link
- Enter your user name in the standard format captured during registration
- Enter your password in the standard format of Case sensitive, Alpha Caps, Alphanumeric, numeric & Char e.g. Test12345@ and click Log In button to proceed.

Caution: Remember to keep your username and password safe.
6. goAML platform landing page

The landing page has the following visible items

- **Logged in user details** - details which user is logged in for which institution (e.g. Sipho from XYZ Bank)[a]

- **Menu Bar** - contains New Reports / Drafted Reports / Submitted Reports / Message Board / My goAML / Admin / Help / Logout. Clicking any of the link item will give a user access to the functionality required (i.e. clicking message board populates the message board)[b]

- **Information Bar** - contains the FIC information with links to download goAML documentation[c]

- **Logout** - allows you to logout as a user[d].

---

[a] (Sipho) XYZ Bank

[b] NEW REPORTS ▼ DRAFTED REPORTS ▼ SUBMITTED REPORTS ▼ MESSAGE BOARD ▼ MY GOAML ▼ ADMIN ▼ [c] LOGOUT

The Financial Intelligence Centre Act 38 of 2001 (the FIC Act) mandates all accountable institutions to submit Cash Threshold Reports (CTR). Furthermore the FIC Act mandates all accountable and reporting institutions to submit Terrorist Property Reports (TPR) and requires all businesses (which include accountable and reporting institutions) to submit Suspicious Transaction Reports (STR) to the Centre in terms of section 28; 28A and 29 respectively. The manner of reporting is prescribed by the Regulations to the Act under section 22. The reporting must be done electronically by means of the Centre’s web-based portal or a batch reporting method.

The Centre has chosen goAML as its preferred IT platform to handle all its reporting, data collection, analysis, and case management and secure communications required for the Centre’s daily operational functions and requirements. The goAML system will in future standardise all report types and also clearly distinguish between activity reports and bi-party (“to” and “from”) transaction reports, and the batch reporting method will be limited to transaction reporting which includes the current CTR, TPR and STR reports. The goAML XML Schema will be utilised by the Centre for all future batch and electronic web-based portal reporting and will have to be adapted and implemented by all of the Reporting entities that file Intelligence reports with the Centre.

goAML is an Integrated software solution developed and maintained by the United Nations Office of Drugs and Crime (UNODC) specifically for use by financial intelligence units (FIUs) internationally and has to date been deployed to twenty one (21) other FIUs. goAML is specifically designed to meet the data collection, management, analytical, document management, workflow and statistical needs of any FIU irrespective of its size. Please refer to UNODC website for further information in relation to the system and related products and services.

Click [here](#) to download goAML specifications and related documents.
7. Capturing a Suspicious Activity Report

7.1 Select a new Report
The link for uploading reports is accessible by hovering the mouse pointer on the menu bar.

- **New Reports > click Web Reports**

Once selected, a general reporting template will be generated.

7.2 Reporting template - overview
The form for creating new reports is loaded and displayed. The form fields Entity and Reporting Person are automatically completed and cannot be changed. The Reporting Person details are linked to the logged in user details.

![Reporting template screenshot](image-url)
BASELINE SCENARIO FIELD A – REPORT TYPE

7.3 Select Report Type

The type of report to be submitted is selectable from the **Type** drop down list, each report type will have unique fields i.e. transactional reports fields will differ from activity report fields.

- To capture a SAR, select from the **Type** drop down list > select **Suspicious Activity Report (SAR)**
Report Type window populates with the following fields:

- **Entity** – Automatically filled in and cannot be changed (Linked to Login ID)
- **Type** – Type of Report (e.g. SAR)
- **Submission Date** – Automatically generated once the report is submitted
- **Reason for Reporting** (mandatory) – free text field to capture additional readily available information relating to the party being reported (eg. KYC information, expected activity etc). This field explains **WHY** the activity is suspicious/unusual.
- **Action** (mandatory) – Action taken (e.g. Reported the activity to Law Enforcement)
- **Reporting Entity Reference**
- **Reporting Entity Branch** – Branch where the transaction took place (mandatory)
- **FIC Ref Number** - This field is for resubmitting failed/rejected reports and needs to reference the original report number issued by the FIC
BASELINE SCENARIO FIELD B – REPORTING PERSON AND LOCATION

7.4 Reporting Person

Reporting Person - Full details of the report’s reporting person automatically filled in (Linked to Login ID).

7.5 Location

Describes the actual geographical area / branch where the abandoned, proposed, cancelled or attempted transaction or series of transaction or suspicious and unusual activity occurred. The address of the logged in user is pre-populated with the address of the registered profile. The logged in user must edit or delete the address if the populated address is not the actual location of where the transaction (series of transactions) / activity occurred. The address is to be completed in full, including the postal code if available.

7.6 Editing the Location

Click the edit icon

- Address form populates > Edit the fields
The “**Use an existing Address**” button is used to populate Address information that was already captured on the web session on goAML;

- **Type** – It can be Business, Operational, Private, Public, Unknown
- **Town** – Name of town / district as part of a city
- **Postal / Zip** – The postal code of the city
- **Province / State** – Name of the province
- **Address** – Physical Address - details like street name, house number etc.
- **City** – Name of the city
- **Country** – Name of the country
- **Comments** – If any

**BASELINE SCENARIO FIELD C – INDICATORS**

**7.7 Indicators**

Indicators are used to specify the nature or type of suspicious or unusual activity the institution is reporting to the FIC. The institution is required to review the list of predetermined indicators on the scroll down list, and select the most appropriate explanation(s). More than one “**Report Indicator**” may be provided. To select the appropriate indicator:

- **Click Add** to select the appropriate indicator for the report
Type in the **Indicator Code or search word** [a] > click **Search Button** [b] > select by checking the **Indicator**[c]> **Close**[d].

- **Or Scroll** > select by checking the **Indicator** > **Close**

- The selected **Indicator** will be displayed on the form. Click **X** to delete the searched indicator

SAR indicators – in terms of section 29 of the FIC Act in respect of prohibitions relating to persons and entities identified by a resolution of the United Nations Security Council (targeted financial sanctions)
Where there is a suspicion that such action or series of actions, relates to the contravention of section 26B of the FIC Act, then the accountable institution, reporting institution or person must report that suspicion to the FIC.

Section 26B prohibits persons and entities identified by the United Nations Security Council from, amongst others, directly or indirectly acquiring, collecting, possessing property, making available property or making it possible for any person or entity referred to in the TFS list (section 26A(1) of the FIC Act) to retain or control property.

Whilst multiple report indicators may be provided, a business rule exists that indicates that a minimum of one report indicator per report must be included.

Note: the above selection of indicator is for demonstration purposes only. The institution is required to review the list and select the most appropriate indicator for the activity being reported.

BASELINE SCENARIO FIELD D – ACTIVITY

7.8 Activity

An Activity form represents an event where a list of subjects (person / account / entity) and goods and services are related directly to the report without the need of a transaction:

- Click Add button to capture activity details for the report and details of the report need to be completed

- Clicking the Activity add button generates the activity form and details of the report need to be completed. Two fields are generated > Report Parties and Goods and Services
<table>
<thead>
<tr>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Parties *</td>
</tr>
<tr>
<td>Goods and Services</td>
</tr>
</tbody>
</table>
BASELINE SCENARIO FIELD E – REPORTING PARTIES

7.9 Reporting parties

Report parties represents a collection of involved subjects (Account (s) / Entity (ies) / Person (s)) for the activity report. To capture the details of the involved parties

- Click Report Parties add button > The Report Party form populates. Complete the reporting party details, at least one party should be included

<table>
<thead>
<tr>
<th>Report Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significance</td>
</tr>
<tr>
<td>Comments</td>
</tr>
<tr>
<td>Party Type</td>
</tr>
<tr>
<td>Person</td>
</tr>
<tr>
<td>Account</td>
</tr>
<tr>
<td>Entity</td>
</tr>
</tbody>
</table>

- Significance - The significance value refers to the scale of involvement of a person If a person’s significance value is 9, it means this subject is highly involved in a proposed, cancelled or attempted transaction or series of transaction or suspicious and unusual activity , whereas, a subject with a value of 2 means the subject is mildly involved

- Reason – Why the subject is involved in the current report

- Comments – If any
BASELINE SCENARIO FIELD F – PARTY TYPE (PERSON / ACCOUNT / ENTITY)

7.10 Party Type

The field party type in an activity report is mandatory; the reporter must indicate whether the party type is a person, account or entity, as the report does not have a From (payee) and To (receiver) side like a transactional report. Party Type has three radio button Person / Account / Entity that are discussed next:

7.11 Person Form

![Radio buttons for Party Type: Person, Account, Entity]

- Click the Person radio button > The Person add button displays > Click the Add button > the Person add button, to generate the Person form

![Person form]

The below screen will generate once the person has been selected. “Use an existing Person” button is used to populate Person information that was already captured on the web session on goAML.
Clicking the Yes radio button populates additional fields to be completed

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>e.g. Ms / Dr / Mrs</td>
</tr>
<tr>
<td>First Name</td>
<td>First name of the person</td>
</tr>
<tr>
<td>Middle Name</td>
<td>Middle name of the person</td>
</tr>
<tr>
<td>Birth Date</td>
<td>Date of birth/ can be typed in ccyy/mm/dd format</td>
</tr>
<tr>
<td>Mothers Name</td>
<td>Maiden Name</td>
</tr>
<tr>
<td>RSA ID Number</td>
<td></td>
</tr>
<tr>
<td>RSA Passport</td>
<td></td>
</tr>
<tr>
<td>Nationality 1</td>
<td></td>
</tr>
<tr>
<td>Nationality 2</td>
<td></td>
</tr>
<tr>
<td>Country of Origin</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Occupation</td>
<td></td>
</tr>
<tr>
<td>Employer Name</td>
<td></td>
</tr>
<tr>
<td>Tax Number</td>
<td></td>
</tr>
<tr>
<td>Tax Reg. Number</td>
<td></td>
</tr>
<tr>
<td>Source of Wealth</td>
<td></td>
</tr>
<tr>
<td>Non RSA ID/Passport?</td>
<td>No / Yes</td>
</tr>
<tr>
<td>Deceased?</td>
<td>No / Yes</td>
</tr>
<tr>
<td>Foreign Passport/Foreign ID/Permit/Refugee</td>
<td></td>
</tr>
<tr>
<td>Issuing Country</td>
<td></td>
</tr>
<tr>
<td>Deceased?</td>
<td>No / Yes</td>
</tr>
<tr>
<td>Date of Death</td>
<td></td>
</tr>
</tbody>
</table>

- Prefix – Any name prefix (e.g. titles of nobility - Duke)
- Birth Place – Place of birth
- Alias / Known As – Also known as name or other aliases
- RSA Passport – South African passport number
• RSA ID No – 13 digit South African ID Number. This is a mandatory field in the event that it is my client and said client has a SA ID Number (e.g. 7404080408069)
• Nationality 1 – The status of belonging to a particular nation, whether by birth or naturalisation
• Country of Origin – The country in which a person is deemed to have originated
• Occupation – Job title of the person
• Gender – Male / Female
• Surname / Last Name – Surname of the reported person
• Tax Number – The tax number of the individual whose details are being captured
• Tax Reg. Number – The person’s tax registration number issued by tax authorities
• Source of Wealth – The source of wealth / income of the individual whose details are being captured (NOTE: As per the Regulations, this is the information relating to Source of Funds)
• Non RSA ID / Passport? – No / Yes
• Nationality 2 – The status of belonging to a particular nation, whether by birth or naturalisation
• Residence – Select the current residence country of the person
• Employer Name – Record of Employer details
• Foreign Passport / Foreign ID / Permit / Refugee / Residence Number – If reported person is not a South African citizen/resident (thus no SA ID Number and/or SA Passport Number) and thus the Non South African Number/Document field is “Yes”, the completion of a Passport / Foreign ID / Permit/Refugee / Residence number is mandatory
• Issuing Country – The country which issued the respective Foreign Passport / Foreign ID / Permit / Refugee / Residence Number
• Deceased – No / Yes, if the person has passed away
• Date of Death – If the person has passed away, then the date of passing is required in ccyy/mm/dd format
7.12 Phone

<table>
<thead>
<tr>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact Type</strong></td>
</tr>
<tr>
<td>e.g. Business</td>
</tr>
<tr>
<td>e.g. Operational</td>
</tr>
<tr>
<td>e.g. Private</td>
</tr>
<tr>
<td>e.g. Public</td>
</tr>
<tr>
<td>e.g. Unknown</td>
</tr>
<tr>
<td><strong>Country Prefix</strong></td>
</tr>
<tr>
<td>e.g. 27</td>
</tr>
<tr>
<td><strong>Extension</strong></td>
</tr>
</tbody>
</table>

- **Contact Type** - It can be Business, Operational, Private, Public, Unknown
- **Comm. Type** - It can be Landline, Mobile, Satellite
- **Country Prefix** - e.g. 27
- **Number** - Numeric, digits (e.g. 0128012556)
- **Extension** - Numeric
- **Comments** - if any

7.13 Address

<table>
<thead>
<tr>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>e.g. Business</td>
</tr>
<tr>
<td>e.g. Operational</td>
</tr>
<tr>
<td>e.g. Private</td>
</tr>
<tr>
<td>e.g. Public</td>
</tr>
<tr>
<td>e.g. Unknown</td>
</tr>
<tr>
<td><strong>Town</strong></td>
</tr>
<tr>
<td>Name of Town / district as part of a city</td>
</tr>
<tr>
<td><strong>Postal/Zip</strong></td>
</tr>
<tr>
<td>the postal code of the city (e.g. 0122)</td>
</tr>
<tr>
<td><strong>Province/State</strong></td>
</tr>
<tr>
<td>name of the province (e.g. Gauteng)</td>
</tr>
</tbody>
</table>

- **Type** - It can be Business, Operational, Private, Public, Unknown
- **Address** - Physical Address - details like street name, house number etc.
- **Town** - Name of Town / district as part of a city
- **City** - Name of the city
- **Postal / Zip** - the postal code of the city (e.g. 0122)
- **Province / State** - name of the province (e.g. Gauteng)
- **Country** - name of the country
- **Comments** - if any
7.14 Identification

<table>
<thead>
<tr>
<th>Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type*</td>
</tr>
<tr>
<td>Issue Date</td>
</tr>
<tr>
<td>Issued by</td>
</tr>
<tr>
<td>Comments</td>
</tr>
<tr>
<td>Number*</td>
</tr>
<tr>
<td>Expiry Date</td>
</tr>
<tr>
<td>Issue Country*</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

- Type – It can be Travel Document / Permit / Passport etc.
- Issue Date – Identification document issue date
- Issued by - Name of authority that issued the document (e.g. Department of Home Affairs)
- Comments – If any
- Number - alphanumeric value of the ID document (e.g. AT08154711 or 8104226008085)
- Expiry Date - The last date of validity of the Identification document
- Issue Country - Country where the document was issued

7.15 Email

<table>
<thead>
<tr>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail Address*</td>
</tr>
</tbody>
</table>

- Email – person’s email address

7.16 Employer Address and Employer Phone

Clicking the Employer Address / Phone add button generates person’s employers form to be completed
7.17 Save and Cancel Button

- **Save** – The save button adds information to the person’s form
- **Cancel** – To cancel or discard the current screen information

7.18 Account

Clicking the **Account** radio button generates **Account field** > click the **Add** button to generate the form

- Whenever the involved **Account / Person / Entity** is the client of the reporting entity, more details may be demanded on the client, and the reporting entity must have the information as part of the adherence to the client identification and verification requirements of the **FIC Act**.
- In the instance of an account of a minor both the details of the minor and guardian authorised to transact on his/her behalf should be captured

The “**Use an existing Account**” button is used to populate **Account** information that was already captured on the web session on goAML.

- **Account Number** - Account number (for **Non-Banking** institution the account number can refer to the client
- **Name** - The type of account that is being referred to- i.e. Trust account, savings account or client account etc.
number/profile number assigned by the institution

- Institution Registration Name - Name of the institution where account is held

- Non Banking Institution? – Yes (if institution is not a bank)
- Code or SWIFT? – Choose Institution Code
- Non Banking Institution? – No (If institution is a bank)
- Code or SWIFT? – Choose SWIFT Code

- Account Type - Type of account (e.g. Trust or Client)
- Currency Code - Currency the account is kept in
- Balance - The account balance at the time of reporting
- SWIFT – SWIFT code according to ISO 9362 (e.g. XYZ001)
- Institution Code – Unique institution code of the entity where the account is held
- IBAN (International Bank Account Number) - is a number attached to all accounts, the code identifies the country the account belongs to, the account holder’s bank and the account number.
- Opened – Date account opened in ccyy/mm/dd format
- Status Code - Account status when transaction was initiated (e.g. Active / Closed)
- Beneficiary - Ultimate beneficiary of the account (Should be completed where the beneficiary is different from signatory)
- Client Number - Client number
- Closed - Date account closed in ccyy/mm/dd format

Please Note: When a branch / business unit / franchise is reporting an account which belongs to a group / head office or other registered reporting entity on goAML - the relevant account must be reported in a standardised format to avoid unnecessary duplication of information.

**Entity**

Clicking the **Entity** add button generates the **Entity** form, the form is used to complete the details of the business entity owning the account, for **Entity** form refer to **7.19**

**Signatory(ies)***

Clicking the **Signatory (ies)** add button generates the **Signatory (ies)** form, the form is used to complete the details of the **Person(s)** with access to the account

- Is Primary - Identifies the primary account holder. Only one signatory may be marked as primary account holder
- Role - The role of the signatory (e.g. Beneficiary, Account Holder)
• Person - populates Person form refer paragraph 7.11

<table>
<thead>
<tr>
<th>Beneficiary Comment</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• Beneficiary Comments – Any special remark on the beneficiary
• Comments - If any

Please Note: In instances where an account has multiple signatories, all of the signatory details need to be captured.

Save and Cancel Button

- Save – The save button adds information to the Account form
- Cancel – To cancel or discard the current screen information

7.19 Entity

Clicking the Entity radio button generates **Entity** field > click the Add button to generate the form

The “**Use an existing Entity**” button is used to populate Entity information that was already captured on the web session on goAML
- Name – Name of the entity
- Incorporation Legal Form - The legal form of the entity
- Incorporation Number - The registration number of the entity / company in the relevant authority (e.g. Chamber of Commerce/ CIPC etc.)
- Incorporation State / Province - Name of the province
- E-mail - Entity email address
- Tax Number – The entity tax number
- Comments – If any
- Business Closed? – Yes / No
- Date Closed – If entity is closed, specify the date of closure in ccyy/mm/dd format
- Registered Name – The Registered name of the institution (CIPC)
- Business – Business area of the entity
- Date Closed – If entity is closed, specify the date of closure in ccyy/mm/dd format
- Incorporation Date - Incorporation registration date in ccyy/mm/dd format
- Incorporation Country Code - Incorporation registration country code, select from a list
- Licence Number - Licence Number issued by the applicable supervisory body as per schedule 2 of the FIC Act
- Reg. Number - Registration Number provided to the tax authority and also extend to include relevant licensing or supervisory registration / trading number provided to the institution
Clicking the **Phones** add button generates the phones form, for **Phone** form refer to 7.12

**Phone**

![Phones add button](image)

Clicking the **Address** add button generates the address form, for **Address** form refer to 7.13 **Address**

**Address**

![Address add button](image)

Clicking the **Director(s)** add button generates the Person (s) form, complete the details of the individual authorised as directories, for **Person** form refer to 7.11 **Persons**

**Director(s)**

![Director(s) add button](image)
7.20 Goods and Services

Clicking the **Goods and Services** Add button generates the **Transaction form**

The **Transaction form** is used to capture the transaction item details

### Transaction Item

<table>
<thead>
<tr>
<th>Item Type*</th>
<th>Item Make</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description*</th>
<th>Previously Registered To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Presently Registered To</th>
<th>Estimated Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Item Type** – The type of item (e.g. Vehicle)
- **Item Make** – Item maker (e.g. if the item is a car - BMW)
- **Description** – Description of the item (e.g. Luxury Car)
- **Previously Registered To** - Name of previous owner
- **Presently Registered To** - Name of current owner
- **Estimated Value** - Estimated value of the item

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Disposed Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>currency Code</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Size UOM</th>
<th>Registration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Registration Number</th>
<th>Identification Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

- **Status Code** – Stats code (e.g. Bought, Hired)
- **Disposed Value** - Effective value for property transfer (e.g. R500 000.00)
• Currency Code – Used to report service conducted in foreign currency
• Size UOM – Unit of measurement (e.g. square meters)
• Registration Number – Official registration number (e.g. Car VIN Number)
• Comments – if Any

Clicking the Address add button generates the address form, for Address form refer to 7.13 Address

Status Comments - If any

7.21 Adding Multiple Parties to Activity Report

• goAML users are able to add multiple parties on a single activity report. To add Multiple Report Parties
• Click the Report Parties Add button field (refer to 5.9) > the Report Party form will populate > complete the details and Save. Captured report parties are editable by clicking the Edit button

7.22 Saving / Submitting the report

Submit Report - SAR reports can be submitted using the Submit Report Button.

Save Report - Save the SAR reports for editing later. The FIC advises that users should save the report whilst completing the various sections and before submission to ensure the draft report is available in the event of a time-out error.

Show Attachments x 0 – documents can only be attached after saving the report, this button must be used to attach documents such as identification document (ID), proof of address, deposit slips, multimedia files and client information.

Please Note: All information must be captured as structured information per report type and no information that should have been captured as structured data may be attached to the report.
7.23 Attaching a document to a saved report

After saving the report your entity will have the following screen visible on goAML:

- Select the “Show Attachments” Button
• A pop-up screen will appear. Select Choose File> Browse> select the file for upload> select “Upload” to save it on the system.

This step can be repeated for multiple attachments to a maximum of 20MB.

• Once the entire report has been completed- please remember to press the “Submit Report” function.
8. Reviewing saved and submitted reports

8.1 Reviewing a saved report

- Login using your user details see paragraph 5;
- Click on DRAFTED REPORTS> Not Submitted Web Reports

- [a] Select the date range for the reporting period required;
- [b] Click on the search icon
• To make amendments to the report, select the “pencil” icon [a]. Selecting this will open the reporting page, as discussed above.

• To delete the report, select the “x” [b]

• To review the report, select the “eye” icon [c]. The report is NOT editable in this view.


### Not Submitted Web Reports

<table>
<thead>
<tr>
<th>Report ID</th>
<th>Report Type</th>
<th>Created By</th>
<th>Last Updated By</th>
<th>Org Name</th>
<th>Transactions</th>
<th>Status</th>
<th>Last Updated On</th>
<th>Days before Cleanup</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>3484135-0-0</td>
<td>Cash Threshold Report Aggregation (CTRA)</td>
<td>Sipho</td>
<td>Sipho</td>
<td>XYZ Bank</td>
<td>0</td>
<td>Not submitted</td>
<td>2017/05/09</td>
<td>15 [a]</td>
<td></td>
</tr>
<tr>
<td>3484134-0-0</td>
<td>Terrorist Financing Transaction Report (TFTR)</td>
<td>Sipho</td>
<td>Sipho</td>
<td>XYZ Bank</td>
<td>0</td>
<td>Not submitted</td>
<td>2017/05/09</td>
<td>15 [b]</td>
<td></td>
</tr>
<tr>
<td>3484133-0-0</td>
<td>Terrorist Financing Activity Report (TFAR)</td>
<td>Sipho</td>
<td>Sipho</td>
<td>XYZ Bank</td>
<td>0</td>
<td>Not submitted</td>
<td>2017/05/09</td>
<td>15 [c]</td>
<td></td>
</tr>
<tr>
<td>3484132-0-0</td>
<td>Terrorist Property Report (TPR)</td>
<td>Sipho</td>
<td>Sipho</td>
<td>XYZ Bank</td>
<td>0</td>
<td>Not submitted</td>
<td>2017/05/09</td>
<td>15 [a]</td>
<td></td>
</tr>
<tr>
<td>3484131-0-0</td>
<td>Suspicious Transaction Report (STR)</td>
<td>Sipho</td>
<td>Sipho</td>
<td>XYZ Bank</td>
<td>0</td>
<td>Not submitted</td>
<td>2017/05/09</td>
<td>15 [a]</td>
<td></td>
</tr>
<tr>
<td>3484130-0-0</td>
<td>Suspicious Activity Report (SAR)</td>
<td>Sipho</td>
<td>Sipho</td>
<td>XYZ Bank</td>
<td>0</td>
<td>Not submitted</td>
<td>2017/05/09</td>
<td>15 [a]</td>
<td></td>
</tr>
<tr>
<td>3484127-0-0</td>
<td>Cash Threshold Report (CTR)</td>
<td>Sipho</td>
<td>Sipho</td>
<td>XYZ Bank</td>
<td>0</td>
<td>Not submitted</td>
<td>2017/05/09</td>
<td>15 [a]</td>
<td></td>
</tr>
</tbody>
</table>

- **Report ID** - reference number automatically assigned to report once saved
- **Report type** – the type of report being reported
- **Created by** – the name of the user who saved the report
- **Last updated by** – the person who amended the reporting information
- **Transactions** – Number of transactions captured (only applicable to transaction reports)
- **Status** – refers to the status of the report
- **Last updated on** – date when last amendments were made
- **Days before cleanup** – details how many days remaining before the system removes this data from the goAML system
- Org Name – the name of the entity the report is being submitted for
- # - provides options to either view, edit or delete the report

8.2 Reviewing a submitted report

- Login using your user details see paragraph 5;
- Click on SUBMITTED REPORTS> Web Reports

![Web Reports]

- [a] Select the date range for the reporting period required;
- [b] Click on the search icon

![Search](SiphO XYZ Bank)

- To review the report, select the “eye” icon [a]
- To save the report, select the “disk” icon [b].

<table>
<thead>
<tr>
<th>Report ID</th>
<th>Report Type</th>
<th>Created By</th>
<th>Last Updated By</th>
<th>Created On</th>
<th>Org Name</th>
<th>Submitting Org</th>
<th>Transactions</th>
<th>Status</th>
<th>Submitted On</th>
</tr>
</thead>
<tbody>
<tr>
<td>4591-0-1</td>
<td>Suspicios and Unusual Activity Report (SAR)</td>
<td>kn_tst</td>
<td>kn_tst</td>
<td>2018/11/02</td>
<td>Test Bank</td>
<td>Test Rank</td>
<td>0</td>
<td>Processed</td>
<td>2018/11/02</td>
</tr>
</tbody>
</table>

- Report ID - reference number automatically assigned to report once saved
- Org Name – the name of the entity the report is being submitted for
- Report type – the type of report being reported
- Created by – the name of the user who saved the report
- Last updated by – the person who amended the reporting information
- Created On – date report was generated
- Transactions - Number of transactions captured (only applicable to transaction reports)
- Status – refers to the status of the report
- Submitted on – date when report was submitted to the FIC
- # - provides options to either view or save the report

The following active status options are available for submitted reports:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Approved or Accepted:</strong> scheduled for processing</td>
<td>The state after the report has been successfully filtered through applying business rules or rejection rules. These rules are applied on the goAML DeskTop client component. The status is then propagated to the web component.</td>
</tr>
<tr>
<td>Archived - accepted</td>
<td>The state of a report archived whilst the report was still in the state of approve or accepted.</td>
</tr>
<tr>
<td>Archived - invalid structure</td>
<td>The state of a report archived whilst the report was still in the state of invalid structure.</td>
</tr>
<tr>
<td>Archived - not submitted</td>
<td>The state of a report archived whilst the report was still in the state of not submitted.</td>
</tr>
<tr>
<td>Archived - reverted not submitted</td>
<td>The state of a report archived whilst the report was still in the state of reverted - not submitted.</td>
</tr>
<tr>
<td>Archived - reverted original copy</td>
<td>The state of an original copy of the report archived whilst it was still in the state of reverted.</td>
</tr>
<tr>
<td>Archived - waiting to be reverted</td>
<td>The state of a report archived whilst the report awaits to be reverted whilst in failed validation or rejected state.</td>
</tr>
<tr>
<td>Failed Filtering</td>
<td>The state of the report reached after the report has failed filtering, i.e. applying business or rejection rules. These rules are applied on the goAML DeskTop client component. The status is then propagated to the web component.</td>
</tr>
<tr>
<td>Failed Integration</td>
<td>The state of the report reached after the report has failed integration, i.e. processing it into the goAML data store. These rules are applied on the goAML DeskTop client component. The status is then propagated to the web component.</td>
</tr>
<tr>
<td>Failed Loading</td>
<td>The state of the report reached after the report has failed bulk loading into the goAML DeskTop client component. The status is then propagated to the web component.</td>
</tr>
</tbody>
</table>

User guide to submit suspicious activity reports (SAR) on the registration and reporting platform of the Financial Intelligence Centre
Version 3.0 | 21 August 2019
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Validation</td>
<td>The state of the report reached after the report has failed XML Schema Definition (“XSD”) validation rules.</td>
</tr>
<tr>
<td>Failed Validation; Invalid Structure</td>
<td>The state of the report reached after the report has failed to comply with XML Schema Definition (“XSD”).</td>
</tr>
<tr>
<td>Filtered; pending approval</td>
<td>The state of the report reached after the report has successful filtering, i.e. applying business or rejection rules. These rules are applied on the goAML DeskTop client component. The status is then propagated to the web component.</td>
</tr>
<tr>
<td>Loaded; pending filtering</td>
<td>The state of the report reached after the report has successful bulk loading of reports. These rules are applied on the goAML DeskTop client component. The status is then propagated to the web component.</td>
</tr>
<tr>
<td>Marked for Rejection</td>
<td>The state of the report reached after the report has successful filtering, i.e. applying business or rejection rules but not approved. These rules are applied on the goAML DeskTop client component. The status is then propagated to the web component.</td>
</tr>
<tr>
<td>Not submitted</td>
<td>The state of the report saved on the website as drafts, i.e. not submitted reports. Applicable for reports that are manually captured via the web.</td>
</tr>
<tr>
<td>Processed</td>
<td>The state of the report reached after the report has completed all steps required successful, and it is the end state for this process. The status is then propagated to the web component.</td>
</tr>
<tr>
<td>Processing</td>
<td>The state of the report reached after the report has successfully been loaded and ready for validation against the XSD.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The state of the report reached after the report has either resulted in an unexpected error or failing approval state.</td>
</tr>
<tr>
<td>Report integration in progress</td>
<td>The state of the report reached after the report has been approved and integration into goAML data store has commenced. This takes place on the goAML DeskTop client component and the status is then propagated to the web component.</td>
</tr>
<tr>
<td>Report Transfer in progress</td>
<td>The state of the report reached after the report has been successfully validated against the XSD and in the process of being transferred to the goAML DeskTop client component.</td>
</tr>
<tr>
<td>Reverted</td>
<td>The state of the report reached after the report has reached the failed validation or rejected. The intent and purpose of this action is to enable users to correct the causes of failures and re-submit.</td>
</tr>
<tr>
<td>Reverted - Not submitted</td>
<td>The state of the report reached after the report has reached the failed validation or rejected. The intent and purpose of this action is to enable users to correct the causes of failures and re-submit.</td>
</tr>
<tr>
<td>Transferred From Web</td>
<td>The state of the report reached after the report has been successfully transferred to the goAML DeskTop client component.</td>
</tr>
<tr>
<td>Unexpected Error</td>
<td>The state of the report reached after the report has encountered errors, during the XSD validation, that were not expected and should be brought to the attention of the FIC.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>Uploaded</td>
<td>The state of the report reached after the report has been successfully uploaded or submitted.</td>
</tr>
<tr>
<td>Validated; scheduled for loading</td>
<td>The state of the report reached after the report has been successfully transferred to the goAML DeskTop client component and ready for bulk processing on the goAML DeskTop client component.</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>XML Bulk Loading in progress</td>
<td>The state of the report reached after the report has been successfully transferred to the goAML DeskTop client component and xml file bulk loading is in progress on the goAML DeskTop client component.</td>
</tr>
</tbody>
</table>
9. Important reporting tips

- Reporting entities are advised to monitor the goAML Message Board and "Submitted Reports" menu to track the progress of their reports. Please await the processing outcome before attempting to resubmit or remediate regulatory reports as this may cause duplication of regulatory reports.
- In the event of a failed/rejected regulatory report the reporting entity must remediate the regulatory report as per the defined process to ensure that they discharge their reporting obligations successfully.
- Always ensure that web reports are saved before submitting it on goAML Web.
- Available attachments (i.e. copy of ID) may be uploaded and submitted with the initial regulatory report submitted to the FIC.
- Download copies of all web reports submitted and save on the reporting entity's internal systems for record keeping purposes.
- Monitor the “Draft Reports” menu - FIC has noticed that many reporting entities have saved regulatory reports as drafts, but have not yet finalised and submitted all regulatory reports (i.e. have not discharged their reporting obligation).
10. Reporting Process workflow
For goAML support contact the FIC:

Log a web query:  
Click [HERE](#) for compliance queries

-ENDS-

Updated and Issued by

The Financial Intelligence Centre

OCTOBER 2017