BUSINESS OVERVIEW

Institute for Restrictive Measures
1 June 2026

Business Overview & User Guide

Defensible sanctions screening, run on your own desktop

You need a clear, defensible record that the people and companies you deal with have been checked against the OFAC (US), UN, UK and EU sanctions lists — but paid third-party services are costly, opaque about how they decide a match, and require sending your subject data to an outside provider. The IRM Sanctions Screener removes all three problems: it talks straight to the issuing authorities, runs on your own Windows desktop, and produces a professional, timestamped PDF audit report for every screening you perform.

AT A GLANCE

What it does

Update

One click pulls the latest official lists straight from the four authorities — OFAC (US), the UN, the UK (OFSI/HMT) and the EU. The lists are cached on your machine, so once you have updated, screenings run fully offline.

Screen

Enter a person or a company. The tool uses fuzzy name matching with alias handling, then weighs identifiers, date of birth or incorporation, and country to confirm or rule out each candidate.

Report

Generate a timestamped PDF audit trail for the case file — the subject screened, the lists used, every match found, and space for reviewer sign-off.

AUDIENCE

Who it's for

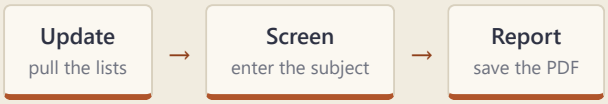
Built for the people who carry the compliance burden but do not want to pay for, or depend on, an outside screening service. If you need a defensible record and full control over your own data, this tool is for you.

Compliance officers · Legal teams · NGOs · Finance staff

- ✓ Onboarding a new client or vendor
- ✓ Periodic re-screening of existing relationships
- ✓ Pre-transaction checks before money moves
- ✓ Building an audit file you can hand to a reviewer or examiner

IN PRACTICE

How a screening works



1. **Update the lists.** Refresh your local copies of the OFAC, UN, UK and EU lists so you are screening against the current designations. After this, no internet connection is needed.
2. **Enter the subject.** Type in the name of the person or company, plus any details you have — an identifier, a date of birth or incorporation, a country. The more you provide, the more confidently the tool can confirm or exclude a candidate.
3. **Review and save.** The tool searches every list and ranks any candidates it finds. You review the results, then save the PDF report to your case file.

Matching is deliberately *fuzzy*, so it catches spelling differences, transliteration variants (the same name written different ways from another alphabet) and known aliases — not just exact text. Where you have supplied them, identifiers, date of birth or incorporation, and country are then used to confirm a genuine hit or rule out a coincidental name clash.

READING THE OUTPUT

Understanding your results

Each candidate is sorted into one of three confidence tiers so you can prioritise your review. The score is how closely the names align.

Tier	What it means	Suggested action
STRONG ≥ 90	Very likely the same party.	Investigate and document the outcome before proceeding.
POSSIBLE ≥ 80	A plausible match that needs a closer look.	Review carefully and record your conclusion.
WEAK ≥ 70	Lower-confidence; often a partial or coincidental name overlap.	Review to exclude, and note why.

The officer always makes the decision. The tool surfaces and ranks candidates for you to assess — it does not clear or block anyone on its own.

THE AUDIT TRAIL

What's in the report — and why it's defensible

Every report is a self-contained record of exactly what was checked, against what, and when. It includes:

- ✓ The exact list version, issuer, record count and download date of every source used
- ✓ A methodology section explaining how matches are found and scored
- ✓ A reviewer sign-off block for the officer's name and conclusion
- ✓ An attribution note — shown only when a backup mirror actually supplied a list

✓ A disclaimer setting out the scope and limits of the screening

Because each report pins down the precise version and download date of every list, you can later demonstrate exactly what data you screened against on a given day — the evidence an audit or regulatory examination asks for.

LISTS SCREENED

Coverage

Five official lists across four authorities, every one fetched directly from the body that issues it:

Authority	Official list
OFAC (US)	Specially Designated Nationals (SDN)
OFAC (US)	Consolidated (non-SDN)
UN	Consolidated List
UK (OFSI/HMT)	OFSI/HMT Consolidated
EU	Financial Sanctions Files (FSF)

PEACE OF MIND

Your assurances

✓ **Your data stays with you.** After an update the tool runs fully offline; subject data never leaves the machine.

✓ **No strings attached.** No subscription, no API key, no vendor lock-in — it talks straight to the issuing authorities, with no third-party sanctions provider in between.

✓ **Nothing hidden.** The matching is transparent, with no concealed filters that could quietly drop a true hit; results are built to be reproduced and defended.

FIRST RUN

Getting started

1. **Launch the app.** Start it the first time with `run.bat`, or open `IRM-SanctionsScreener.exe` once it is built.
2. **Update the lists.** On the **Lists** tab, click **Update** to pull the current lists from all four authorities.
3. **Run a screening.** On the **Screen** tab, enter the subject's details and run the screening, then review the ranked results.
4. **Keep the report.** Save the generated PDF and file it with your case records.

GOOD PRACTICE

Update the lists before any important screening so you are checking against current designations. Set your reviewer name once so it appears on every report. And always keep the PDF in the case file — it is your evidence of what was checked, and when.