

# Iranian Linked Sanctions

## Quick Reference Guide – March 2026

Whilst the current war in the Middle East continues, one of the primary ways you can help protect both the country you live in and your organisation is to make sure you are screening against all Iranian linked Sanctions. Ongoing developments underscore how quickly the situation is evolving – and how interconnected the risks have become.

A key watchpoint is the likely shift in regulatory dynamics. Continued escalation may drive broader and more aggressively enforced sanctions on Iran, particularly targeting Iranian-linked financing networks. This will increase the risk of inadvertent exposure, as the growing use of intermediaries, front companies, and third-country trade routes makes due diligence more complex while raising compliance expectations.



## Take Action Now

### – Protect Both Your Organisation and the National Security Risk.

One of the key risks right now is around corporate concealment, whereby sanctioned individuals and entities look to set up businesses in Gulf states (often with local CEOs and Directors), so that they can dress up in national robes to present themselves as a legitimate entity with no links to any Sanctions and continue their illicit activities. Iranian affiliates, intermediaries, and financiers are increasingly relying on corporate concealment and complex ownership structures to operate expansive shadow banking networks that evade sanctions, facilitate illicit oil trade, and support regional proxy activity.

Authorities have taken note with governments across the GCC as well as the US, UK & Europe targeting these networks directly. Businesses must take note, as not only does allowing these corporate networks to take root present a material national security risk, but a clear compliance risk as well. **We all have specific legal responsibilities and the penalties for inaction can be severe.**

Iranian sanctions are among the most complex and rapidly evolving compliance regimes in the world. This guide distils the core legal requirements and penalties for inaction across all of our clients' core jurisdictions. If there are other countries you would like this analysis on, please let us know.

## Core Compliance Principles

### Continuous screening

You are **legally required** to monitor all of your clients, suppliers and 3rd party relationships against regional sanctions lists. To align with global best practices, we strongly recommend screening against OFAC, EU, and HMT lists, as well as any jurisdictions where you maintain operations or a client base.

### Trace the Owner

You should immediately cease doing business with any entity that is 50% or more owned, directly or indirectly, by a sanctioned party. This includes cases of aggregate ownership, where multiple sanctioned parties collectively hold a 50% or greater stake.

### Understand the Threat

Ensure teams are equipped with up-to-date awareness and training on evolving sanctions risks and circumvention typologies

### \$ = US Rules

Any transaction touching the US financial system falls under US jurisdiction, regardless of local law and so requires OFAC screening.

# Legal Requirements to Comply

Organisations across all jurisdictions are legally required to implement the following. Requirements vary by country but all share core obligations around screening, ownership tracing, reporting, and end-use verification.

Country	Action Required	Sanctions to Follow	Legal Requirements
<b>Bahrain</b>	Automated sanctions screening & monitoring of all of your clients, suppliers and 3 <sup>rd</sup> parties.	CBB Rulebook (Financial Crime), UN Snapback.	Freeze and notify CBB within 24 hours; annual compliance attestation; follow CBB's "Wider Approach" to CDD.
<b>Channel Islands</b>	Full database scrubbing; verify "Control" beyond 50% ownership; monitor local fiduciary structures.	UK Sanctions List (mirrored via local Law, e.g., SAFL 2019).	Direct mirroring of UK OFSI list; report to local FIUs; criminal liability for "enabling" circumvention.
<b>Iraq</b>	Strict Dollar flow vetting; screening of all "Wire Auction" participants and BUNA users.	UN Snapback, CBI Regulations, US Fed (USD) Restrictions.	Strict compliance to avoid US "redlining" of local banks.
<b>Jordan</b>	Transaction monitoring; focus on exchange houses and regional remittance flows.	UK Autonomous (Sanctions Act 2018), UN Snapback, US Secondary.	Implement CBJ-mandated countermeasures; monitor for Iranian "Front Companies" in regional trade.
<b>KSA</b>	Zero-tolerance screening; monitor for IRGC-affiliated logistics; strict UBO tracing.	SAMA/CMA Directives, UN Snapback, Saudi Anti-Terrorism Law.	Compliance with SAMA AML/CFT circulars; reporting matches via the Hemaya system; strict vetting of NGOs.
<b>Kuwait</b>	Enhanced Transaction Monitoring; focus on trade-based money laundering (TBML) risks.	UN Snapback, CBK Circulars, FATF "Call for Action" (High Risk).	Apply countermeasures per FATF Rec 19; report suspicious Iranian-linked flows to KFIU; rigorous KYCC.
<b>Lebanon</b>	Scrub of "Shadow Banking"; screen for Hezbollah/IRGC-linked NGOs and charities.	BDL Circular 126, US Secondary (HIFPAA), UN Snapback.	Adhere to BDL Decision 13790; strict identity verification for all Electronic Payment Service providers.
<b>Oman</b>	Logistics/Shipping screening; monitor for "Ship-to-Ship" (STS) oil transfer alerts.	UN Snapback, CBO Directives (BM/60/8/2025).	Mandatory asset freezing for UN-designated persons; focus on Targeted Financial Sanctions (TFS) for Iranian proxies.

Country	Action Required	Sanctions to Follow	Legal Requirements
<b>Qatar</b>	Enhanced UBO tracing; screening for "Dual-Use" technology; Adverse Media for shell entities.	UN Snapback, QCB/QFC Guidance, FATF Call for Action.	Asset freezing of UN-designated entities; report to QFIU; focus on vetting humanitarian "White Channels."
<b>Syria</b>	Highest Risk/Total Block; monitor for "Triangular Trade" bypassing Western sanctions.	FATF Blacklist, UN Snapback, US Caesar Act.	Strict prohibition of most transactions; monitor for "Ghost Fleets" using Syrian ports for Iranian cargo.
<b>UAE</b>	Automated screening of UN/Local lists; EDD on trade finance/shipping; PEP & Adverse Media.	UAE Local Terrorist List, UN Snapback (Res 1737/2231 legacy).	Register on goAML; freeze assets "without delay" (24-hour window); report Confirmed/Potential matches.
<b>UK</b>	Real-time screening & transaction monitoring for indirect benefits; EDD on complex ownership structures.	UK Autonomous Sanctions Act 2018, UN Snapback, US Secondary.	Immediate asset freeze; report matches/breaches to OFSI; mandatory reporting for relevant firms.

Global	Action Required	Sanctions to Follow	Legal Requirements
<b>FATF Guidelines for All Countries</b>	<ol style="list-style-type: none"> <li>Automated sanctions screening &amp; monitoring of all of your clients, suppliers and 3<sup>rd</sup> parties.</li> <li>Enhanced Due Diligence (EDD): Apply rigorous scrutiny to all Iranian-linked business relationships.</li> <li>Countermeasures: Prohibit or limit correspondent banking; refuse establishment of any direct or indirect link with Iranian bank, branches/ subsidiaries.</li> <li>Transaction Monitoring / Sanctions Screening: Implement systematic Transaction Monitoring and Sanctions / Adverse Media screening of all financial transactions with a nexus to Iran.</li> <li>STR/SAR Filing: Mandatory filing for any activity suspected of Proliferation Financing (PF) or Terrorist Financing (TF).</li> </ol>	<ol style="list-style-type: none"> <li>UNSC Consolidated List: (Particularly restored entries under Resolution 1737 following the 2025 snapback).</li> <li>National/Regional Lists: (e.g., U.S. OFAC SDN, EU Restrictive Measures, UK HM Treasury).</li> <li>FATF Public Statement: Monitoring the "Call for Action" list.</li> </ol>	<ol style="list-style-type: none"> <li>FATF Recommendation 19: Mandatory application of effective and proportionate countermeasures.</li> <li>UNSC Resolution 2231 (Snapback): Legally binding restoration of previously lifted UN sanctions on oil, banking, and arms.</li> <li>FATF Recommendation 7: Strict implementation of Targeted Financial Sanctions (TFS) to prevent proliferation</li> </ol>

# Non-Compliance and Consequences

Given sanctions evasion and corporate concealment are viewed by governments, law enforcement agencies and FIUs around the world as a threat to national security, the penalties for inaction can be severe and debilitating for any business, regardless of what sector you are in.

The table below shows the specific consequences where organisations fail to comply with the legal requirements above. Wilful blindness (i.e. arguing that you didn't know) is no longer a defence and governments are cracking down hard on companies that don't have the right systems and controls in place to detect any potential sanctions links.

Country	Targeted Penalties	Other Macro Risks
<b>Bahrain</b>	Significant financial penalties; criminal prosecution under AML/CFT Decree-Law No. 4.	Blacklisting from the GCC Interconnected Financial System; maritime seizure of vessels/cargo.
<b>Channel Islands</b>	Unlimited fines; custodial sentences; immediate revocation of fiduciary or banking licences.	Total reputational collapse in the global offshore sector; loss of correspondent banking links to London.
<b>Iraq</b>	Permanent ban from the CBI USD Wire Platform; asset seizure.	Designated as a 'Section 311' entity, isolating the company from the global financial grid.
<b>Jordan</b>	Heavy administrative fines; prison terms for 'willful blindness' under Law No. 20.	Secondary sanctions risk – inability to clear transactions in US Dollars.
<b>KSA</b>	Severe statutory fines; permanent debarment from all Government/Vision 2030 contracts.	Assets frozen under national security laws; immediate termination of regional joint ventures.
<b>Kuwait</b>	Unlimited fines; strict administrative penalties from the Kuwait FIU; jail time.	Tiered de-risking – local banks close all associated accounts to protect US relationships.
<b>Lebanon</b>	Immediate freezing of all personal and corporate accounts; loss of banking secrecy protections.	Permanent exclusion from the SWIFT network; loss of credit facilities from international lenders.
<b>Oman</b>	Monetary penalties; criminal prosecution for violating Royal Decrees on UN compliance.	Suspension of Free Zone benefits; loss of the country's neutral mediator commercial status.
<b>Qatar</b>	Fines of QAR 10 million+; revocation of QFC/QCB licences; criminal liability for CEOs.	Loss of access to Western energy technology and international investment partners.
<b>Syria</b>	Near-total asset seizure; criminal charges under the US Caesar Act (extraterritorial).	Primary SDN designation by OFAC – making the company a global pariah for all trade.
<b>UAE</b>	Fines exceeding AED 5 million; closure of business premises; potential deportation of non-national managers.	Re-listing on the FATF Grey List, triggering mass de-risking by international banks.
<b>UK</b>	Criminal fines up to £1 million or 50% of breach value; up to 10 years imprisonment for directors.	Withdrawal of professional indemnity insurance; public naming and shaming by OFSI.

## Non-Compliance Risk Spotlight: Secondary Sanctions & Extraterritorial Reach of U.S.

U.S. sanctions can extend beyond U.S. borders, exposing non-U.S. companies to enforcement even where there is no direct U.S. nexus. Through secondary sanctions, U.S. authorities may penalise foreign entities that engage in certain dealings with sanctioned parties or sectors, including restricting access to the U.S. financial system or imposing designation.

This creates a heightened non-compliance risk for organisations operating internationally. Activities that may be permissible under local frameworks can still trigger U.S. enforcement exposure. Businesses should therefore assess not only their direct counterparties, but also downstream relationships, ownership structures, and transaction flows to identify potential indirect links to sanctioned actors.

Key takeaway: Sanctions compliance must be approached with a cross-jurisdictional lens – failure to account for U.S. secondary sanctions and extraterritorial reach can result in significant financial, operational, and reputational consequences.

## How Tathabbat Powered by Themis can Help

### Static compliance approaches are no longer sufficient.

The good news is that Tathabbat Powered by Themis can help you automate your sanctions screening right away, without any work required by your team, and no disruption to your business. Sign up to our ongoing monitoring service and we will take care of everything so you can rest at night confident that all of your clients, suppliers and 3rd parties are being screened on an automated overnight batch screening process.

Tathabbat Powered by Themis provides the intelligence, investigative capability, and technology to help organisations navigate the Iran sanctions landscape with confidence – from initial risk assessment through to ongoing monitoring and incident response.

What You Need to Do	When?	How Tathabbat Powered by Themis Can Help
<b>Ongoing Monitoring</b>	Immediately	Using our AI-driven Tathabbat Powered by Themis Search platform, you can monitor all of your existing clients, suppliers and 3rd party relationships on an automated overnight batch screening basis. The platform integrates into your existing infrastructure or operates standalone, covering adverse media, regulatory enforcement, and all key sanctions lists in a single automated solution.
<b>Assess sanctions exposure across jurisdictions</b>	As soon as possible	Tathabbat Powered by Themis can help you to ascertain your business specific risk exposures to Iranian Sanctions via a digital Sanctions risk assessment across your business to map exposure across UNSC, US, UK, EU, and international regimes – helping organisations understand where risks may arise as the conflict evolves.

## What You Need to Do

## When?

## How Tathabbat Powered by Themis Can Help

### Strengthen due diligence on counterparties and intermediaries

Within 3 months – for all new clients, suppliers or 3rd party relationships.

Our platform provides real-time sanctions screening, but where there are particularly opaque or complex structures, clients can call in our human intelligence team to perform a deep dive investigation into any given person, company, entity, sector or geography to understand if there are hidden links to Iranian sanctioned networks.

### Monitor emerging evasion tactics

Case by case basis

Threat intelligence identifying evolving Iranian tactics – including front companies, shadow banking, and trade-based schemes – so businesses can update controls accordingly. With its robust AI engine and analytical dashboards, Tathabbat Powered by Themis intelligence can assist with emerging risks to prepare and equip the institutions beforehand with surfacing threats.

### Review supply chains and trade relationships

Within 3 months

Supply chain mapping to identify exposure to high-risk goods, sectors, and logistics routes targeted for sanctions evasion or illicit trade.

### Prepare for rapid regulatory or sanctions changes

Ad-hoc and case by case basis

Ongoing monitoring of ground-level developments and regulatory changes, enabling businesses to anticipate sanctions shifts and adjust compliance frameworks quickly. Tathabbat Powered by Themis can help with learning and awareness requirements for your teams to make them abreast of the latest regulatory requirements and international best practices.

### Develop a proactive risk management strategy

2 to 3 months for a new policy, procedures and SOP devising and case by case for reviews

Intelligence-led risk management integrated into compliance programmes – including scenario planning, policy review, and operational guidance. On demand and regular review of internal policies and procedures to get aligned with prevailing regulatory requirements and a robust tone from the top framework.

**We would encourage all of our key clients, suppliers and partners to take action NOW.**

**These are important steps to protect both your organisation and the elevated national security risks in these times of conflict.**

**The good news is that it is really easy to take action and Tathabbat Powered by Themis can implement this immediately and do all the work for you.**

# Iran Sanctions Risk Support

Is your business covered?

As regional tensions evolve and Iran-related sanctions risks increase, firms must act quickly to protect their business and meet legal responsibilities and regulatory expectations.

Tathabbat Powered by Themis has developed a rapid support package to help organisations screen and monitor clients, counterparties and exposures as sanctions and risk indicators change.

Failure to implement appropriate controls can lead to severe penalties, including fines up to £1 million or 50% of breach value; up to 10 years imprisonment for directors.\*

*\* Penalties will vary across the globe*

Support Includes:

## Sanction Jurisdictional Risk


- What is changing in the Iran sanctions landscape
- Key risks firms should focus on now
- Regulatory expectations and compliance obligations


## Ongoing Monitoring


- Continuous monitoring of clients and counterparties
- Real-time alerts on sanctions and emerging risk indicators
- Dedicated analyst support for escalation and oversight

**In periods of geopolitical uncertainty, Tathabbat Powered by Themis provides the intelligence and monitoring firms need to stay compliant and protected.**

**We can get this set up for you immediately – get in touch and we'll take care of the rest.**

 UK: +44 (0) 20 8064 1724 | UAE: +971 (0) 2 676 7453

 [info@tathabbat.ai](mailto:info@tathabbat.ai)

 [tathabbat.ai](https://tathabbat.ai)



Manama | Riyadh | Abu Dhabi | Dubai | London

© Copyright 2026 | Tathabbat Powered by Themis. | All rights reserved.

