THEMIS

IRAN

COUNTRY RISK BRIEFING 2026

WEARETHEMIS.COM

Country Overview

Location:
Middle East, located in Western Asia; Borders the Caspian Sea to the north, the Persian Gulf and Gulf of Oman to the south, and shares land borders with Iraq, Turkey, Armenia, Azerbaijan, Turkmenistan, Afghanistan, and Pakistan.

Capital:
Tehran

Currency:
Iranian rial (IRR)

Population:
Approx. 92.4 million (2025 UN estimate)

Unemployment Rate:
8.1% (2024 World Bank estimate)

GDP:
GDP $436.91 billion (2023 World Bank estimate)

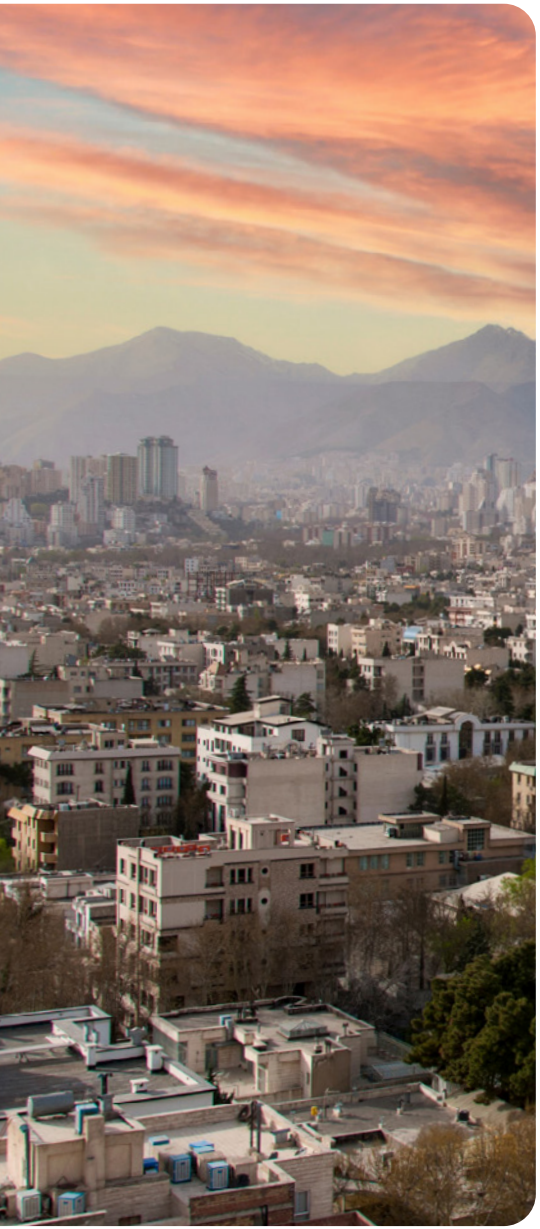
Government:
Theocratic republic, ultimate political authority held by Supreme Leader; dual political structure with elected government including president and parliament (Majles).

Education:
Iran has relatively high literacy rates and a strong emphasis on education, including in science and technology, though the country also faces challenges (e.g. brain drain, sanctions affecting research and education).

Major Economic Sectors:
Hydrocarbon sector (oil, gas, and petrochemicals), services sector (including trade, finance, and technology), industrial sector (manufacturing, construction, and mining), agriculture.

Natural Resources:
Oil and natural gas, coal, copper, iron ore, chromium, zinc, lead, sulphur.

High Financial Crime Risks:
Sanctions evasion, terrorist and proliferation financing, money laundering, trade-based money laundering, cyber-enabled crimes.



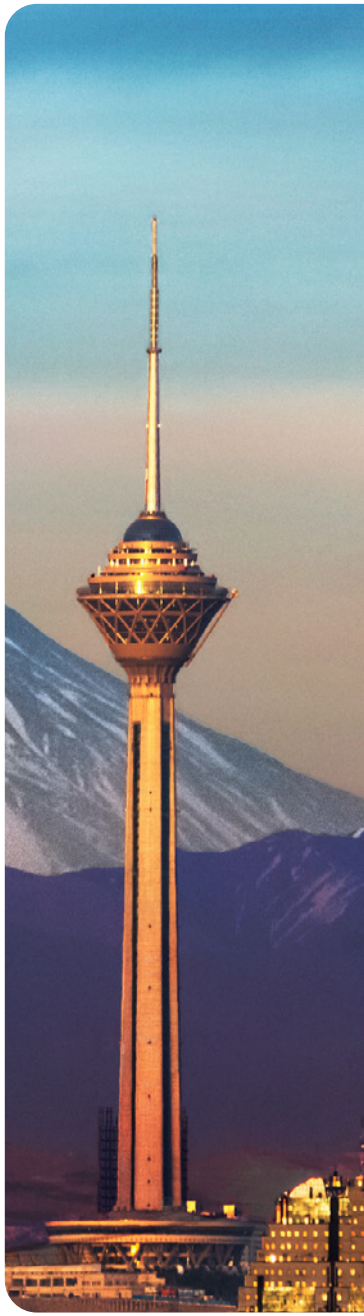
T A B L E O F

Contents

Country Overview	8
Economy & Politics	10
Themis Expert View	13
Financial Crime Risk Matrix	14
Regulatory Overview	30
Financial Action Task Force Assessment	32
Sanctions Landscape	32
Threat Spotlight – Sanctions Circumvention Through Company Formation and Trade Structuring	32
Case Studies	32
Areas of Financial Crime Vulnerability	32
Financial Crime Risk Overview	32
Key Financial Crime Watchpoints	32
Next Steps: Navigating the 2026 Iran Risk Landscape Economy & Politics	32

WWW.WEARETHEMIS.COM

Economy & Politics



Iran, officially known as the Islamic Republic of Iran, is a country in the Middle East characterised by its vast geographical diversity and deep historical roots. Bordered by the Caspian Sea to the north and the Persian Gulf and Gulf of Oman to the south, Iran occupies a strategic position that has shaped its cultural and political significance, with the country home to one of the world's oldest continuous civilisations. Its landscape ranges from arid deserts to rugged mountain ranges, contributing to a wide range of climates and ecosystems.

Iran is one of the Middle East's largest economies, with the capital Tehran serving as the nation's key economic and political hub. The country has substantial hydrocarbons reserves and a diversified industrial base spanning petrochemicals, automobiles, metals, and agriculture. Despite its significant natural wealth, Iran's economic potential has been constrained in recent decades by extensive international sanctions, structural inefficiencies, high levels of corruption, and governance challenges and instability.

Iran's economic situation has deteriorated markedly since 2024, with accelerating inflation, a sharp depreciation of the rial to historic lows, and declining household purchasing power. Limited periods of growth linked to oil exports have been offset by this macroeconomic instability, as well as by energy and water shortages, and widespread labour unrest, further undermining long-term investment and economic resilience.

Politically, Iran functions as a theocratic republic in which the Supreme Leader holds ultimate authority, overseeing the judiciary, security services, and key economic entities. Elected bodies — including the presidency and parliament — operate within a political framework shaped by a Guardian Council and other oversight institutions. Civil liberties are largely restricted, with periodic crackdowns on dissent and limitations on media freedom and political participation.

Iran's modern geopolitical trajectory stems from the 1979 Islamic Revolution, which overthrew the Western-backed monarchy of Shah Mohammad Reza Pahlavi and replaced it with a theocratic state under Ayatollah Khomeini. The revolution fundamentally reoriented Iran's foreign policy away from alignment with the US and other western countries and towards an ideology of resistance to Western influence and support for Islamist movements across the region.

Iran has faced geopolitical isolation and volatility for decades. Coordinated international sanctions against the regime have been in place to varying degrees since the early 2000s. Tensions between Iran, Israel, and the US has steadily intensified through a series of direct and indirect confrontations in recent years. The period between 2024 and 2025 saw increasingly open exchanges of missile and drone attacks between Israel and Iran, alongside Israeli strikes targeting Iranian military infrastructure and personnel in Syria and suspected nuclear-related facilities inside Iran. Diplomatic tensions also rose amid ongoing disputes over Iran's nuclear programme and concerns from the US and other western countries about Iran's expanding missile capabilities. These developments contributed to a steadily deteriorating security environment in the Middle East, with each cycle of retaliation raising the risk that a broader conflict could emerge.

Alongside these direct confrontations, Iran continued to rely heavily on its network of regional proxy groups to project influence and apply pressure on its adversaries. Iranian-aligned actors, including Hezbollah in Lebanon, Shiite militias in Iraq, and Houthi forces in Yemen, carried out periodic rocket, drone, and maritime attacks targeting Israel, US forces, and regional partners in the Gulf. While these groups often operate with varying degrees of autonomy, they are widely viewed as a central component of Iran's regional security and political strategy.

The 2026 Iran Conflict: Key Developments and Regional Implications

On 28 February 2026, the US and Israel launched coordinated airstrikes against Iran in a large-scale operation targeting the country's military infrastructure and political leadership. The strikes hit sites across Tehran and other major cities, marking one of the most significant direct military confrontations between Iran and Western-aligned forces in decades. Iranian Supreme Leader Ayatollah Ali Khamenei and several other senior political and military figures were killed during the initial phase of the operation, triggering a rapid escalation across the region.

In the days following the strikes, hostilities have intensified with Iranian forces launching waves of missile and drone attacks targeting neighbouring Gulf states, Israel, and US military bases in the region. At the same time, the US and Israel have continued strikes on Iran, as well as Israel carrying out a campaign against Hezbollah in Lebanon. As a result, the conflict has rapidly taken on a broader regional dimension. Iranian missiles and drones continue to target Gulf countries, which have caused casualties among civilians and military personnel, as well as disruptions in daily life, trade routes, and economic activity.

Critical infrastructure, including ports, energy facilities, and industrial hubs, has been hit across the region, including Bahrain's state oil company declaring its refinery caught fire in an Iranian attack. Iran's attacks on Amazon data centres in UAE and Bahrain also signal a new kind of threat as technology plays an increasingly strategic role in international conflict. The spillover effects of the conflict are amplifying regional economic uncertainty, slowing trade, and raising the cost of security and insurance, highlighting the broader toll on ordinary people and businesses across the Gulf. The conflict has also generated significant global economic repercussions. Energy markets reacted immediately to the outbreak of hostilities, with oil prices surging above $100 per barrel amid fears of disruption to shipping routes through the Strait of Hormuz, one of the world's most critical oil transit chokepoints. Analysts have warned that any sustained disruption to energy infrastructure or maritime traffic in the Gulf could have substantial knock-on effects for global inflation, energy markets, and supply chains.

Political messaging from the US has emphasised both deterrence and military objectives, with President Trump stating that strikes will continue as necessary to neutralise Iran's missile capabilities and prevent the development of nuclear weapons, framing the campaign as the culmination of an ongoing confrontation rather than the start of a new war. Iranian leadership has responded with equally forceful rhetoric, characterising the strikes as an act of aggression and vowing continued retaliation until its conditions are met. Iran has also signalled its continued willingness to leverage economic pressure if US and Israeli operations continue, most notably threats to further disrupt energy exports by continuing to restrict activity through the Strait of Hormuz, a crucial passage for the global oil trade.

Domestically, Iran is now navigating a period of acute political uncertainty and economic strain. In early March, Mojtaba Khamenei, the son of former Supreme Leader Ayatollah Ali Khamenei, was appointed as his father's successor. Mojtaba Khamenei is widely regarded as an influential figure within Iran's political and security establishment, with longstanding ties to the Islamic Revolutionary Guard Corps (IRGC) and a reputation for exerting significant influence behind the scenes in military and security matters. His appointment signals an attempt by Iran's political and clerical establishment to maintain continuity within the country's leadership structure amid a rapidly evolving conflict environment. The US government has expressed disappointment with Mojtaba Khamenei being chosen as successor.

At the time of this report's writing in March 2026, the situation remains highly fluid. Continued airstrikes inside Iran, ongoing missile exchanges, and the growing involvement of regional actors suggest the potential for further escalation, while the economic and security impacts are already being felt across the Middle East and in global markets.

We're issuing weekly Conflict Advisory Notes to help our community stay informed amid the conflict. These weekly briefs are designed to cut through the noise of 24/7 headlines and breaking updates to deliver clarity on what matters from a financial crime perspective. Our goal is to give you actionable insights and context you can trust, helping you anticipate and respond to the operational, financial, and governance challenges posed by this conflict.

See here for more information on these briefings.

Themis Expert View

WRITTEN BY:

Eliza Thompson

Financial Crime Researcher

2026 Threat Landscape: Iran hosts a deeply entrenched financial crime ecosystem. Regime-linked actors play a central role in sanctions circumvention and proliferation financing, while domestic and regional transnational criminal networks reinforce these channels and participate in a range of other illicit activities. Together, these actors have created a sophisticated and highly resilient threat landscape. Against the backdrop of economic and political turmoil, intensified international sanctions, and ongoing regional conflict, any exposure (whether direct or indirect) to Iranian-linked directors, companies or entities presents acute sanctions risk and heightened financial crime risk.

Organisations should implement enhanced due diligence to identify and mitigate potential exposure, particularly businesses operating in the Gulf and wider region, where cross-border trade, corporate and financial mechanisms, and complex intermediary networks heightened risk exposure. Due diligence should include rigorous scrutiny of counterparties and their extended networks, verification of beneficial ownership structures, and ongoing monitoring for emerging threat indicators that may signal indirect links to Iranian entities.

For decades, Iran has been exposed to significant money laundering and terrorist financing risks. Illicit networks have supported transnational criminal groups and designated organisations such as Hezbollah, Hamas, and various regional militias. The IRGC - Iran's military force – has allegedly leveraged front companies, charities, financial intermediaries, and complex cross-border transactions to move funds and obscure their origin. These activities feed directly into regional instability, with sanctions evasion, trade-based schemes, and shadow-banking networks financing proxy operations, arms procurement, and other destabilising activities across the Middle East.

Iran's energy, mining, logistics, and financial sectors are not only central to the country's economy but also regularly exploited for illicit activity. In particular, the country's oil sector faces high-risk exposure due to strict international sanctions, with intermediary networks and trade-based schemes widely used by the regime to circumvent restrictions. The ongoing economic and geopolitical crisis, coupled with intensified global scrutiny, has further increased dependence on these tactics and the opaque trading and remittance channels that sustain them.

Moreover, Iran's financial isolation and exposure to regional organised crime and instability have turned the country into a testing ground, of sorts, for new laundering and evasion tactics. A 2025 FinCEN advisory, for example, highlighted the scale of Iran's contemporary "shadow banking" networks, which include exchange houses within Iran and front companies abroad that launder billions in oil revenue and help finance military and proliferation programmes. Recent reports suggest these networks have adapted to intensified sanctions and scrutiny, increasingly exploiting cryptocurrencies, alternative digital payment systems, and novel trade-based mechanisms to move funds covertly. For instance, Iran's central bank appears to have used vast quantities of the cryptocurrency Tether to bypass the global

banking system, acquiring $507 million in the stablecoin in 2025 alone.

In addition to these financing channels, non-profit organisations (NPOs) and charities linked to Iran have been notable instruments used by the Iranian regime and proxy actors in moving funds globally. Many of these entities have extensive networks of Iranian expatriates or proxy actors, ostensibly raising money for religious, cultural, or domestic development purposes. While many of these activities are legitimate, intelligence and financial investigations have shown that often significant portions of these funds are diverted to support military projects and proliferation-related programmes. By blending charitable giving with covert financial flows, these organisations can exploit gaps in international oversight and sanctions regimes, effectively functioning as a parallel conduit for Iran's global financial activities. This duality, between legitimate social outreach and illicit financing, makes detecting and disrupting such networks especially challenging for regulators and financial institutions.

Establishing front companies abroad has become a core tactic for some Iranian entities and state-linked actors seeking to maintain access to global markets and circumvent sanctions. While jurisdictions with weaker oversight remain common targets, an increasing number of illicit networks are deliberately setting up entities in countries with strong AML/CTF frameworks, especially countries with leading financial and business ecosystems. Illicit actors are increasingly targeting these jurisdictions to cultivate a veneer of legitimacy by operating within highly regulated environments. Paradoxically, illicit networks in these well governed jurisdictions can actually be more difficult for regulators, financial institutions, and international partners to detect and disrupt, as the businesses often appear compliant and legitimate on the surface.

These companies not only often appear legitimate on paper and may even be managed or incorporated by intermediaries, creating both financial and corporate insulation. In practice, however, they operate as front companies used to conduct business or trade on behalf of sanctioned individuals or entities. Heightened international awareness and increased targeted sanctions against IRGC-linked networks have reportedly made these front structures even more instrumental.

More often than not, businesses engaging with such front companies are unaware of the true beneficiaries behind them. This means that for businesses operating in today's interconnected markets, the risk of inadvertently engaging with a sanctions-evading front company is a very real concern. Even routine commercial transactions can carry hidden exposure, particularly in sectors with elevated exposure due to complex supply chains and commercial structures, such as energy, logistics, commodities, engineering, pharmaceuticals, and technology sectors.

Compounding the challenge, Iranian-linked illicit-finance networks have developed deep, symbiotic ties with specific transnational criminal networks and foreign state-linked actors. IRGC-linked operators reportedly work closely with networks in countries such as China and Russia, exploiting shared vulnerabilities to sanctions and international scrutiny to move and launder funds, traffic restricted goods, and facilitate proliferation financing. This hybrid structure creates a highly opaque ecosystem, significantly complicating enforcement efforts and obscuring risks across global supply chains.

Through sustained investment in illicit financial schemes and adaptive trade-based tactics, Iranian actors have also continually expanded their networks and geopolitical influence. Emerging technologies, including blockchain, AI, and advanced analytics, are rapidly reshaping this landscape, creating new channels for illicit finance and making cross-border flows increasingly difficult to detect and control.

What Does This Mean for Your Entity?

Effectively managing risk in this environment requires a threat-focused approach grounded in practical, operational understanding and real-time insights: not only recognising the typologies that illicit actors employ in Iran, the sectors they infiltrate, and the cross-border networks they leverage, but also understanding how these dynamics change in light of ongoing domestic and international pressures.

Businesses considering engagement with Iranian partners, or operating in markets exposed to Iranian illicit-finance networks — particularly in high-risk sectors such as oil, shipping, logistics, and finance — must adopt a highly cautious and methodical risk posture, carefully assessing both direct and indirect exposure, as well as evolving regulatory and sanctions risks across multiple jurisdictions.

The first imperative for any business is to establish with absolute clarity whether a proposed activity is legally permissible in the jurisdictions where it would occur. For companies operating under U.S., UK, and EU jurisdictions, this challenge is particularly acute due to strict sanctions and compliance requirements that go beyond general AML/CTF obligations. Financial institutions and corporate entities in these regions are subject to rigorous sanctions regimes, requiring enhanced due diligence, comprehensive screening for restricted parties, and proactive reporting of suspicious activity.

In the US, regulations under the Office of Foreign Assets Control (OFAC) and related AML statutes mandate that companies block dealings with sanctioned Iranian entities and maintain robust compliance frameworks to prevent inadvertent violations. Similarly, the UK and EU enforce expansive sanctions lists and require firms to integrate sanctions risk into AML/CTF monitoring, including restricting correspondent banking relationships and applying risk-based reviews for transactions involving high-risk counterparties.

Even for businesses in jurisdictions without direct sanctions against Iran, sanctions risks remain substantial. Certain UN and international restrictions still apply, and the extraterritorial reach of US sanctions can expose entities that engage indirectly with Iranian counterparties or facilitate transactions in US dollars. Companies must therefore assess not only local regulatory requirements but also international obligations and the potential downstream impact on global operations, reputational standing, and financial liability. A proactive, jurisdiction-aware compliance strategy that can adapt to rapid geopolitical and regulatory changes is critical in this environment.

Beyond sanctions, businesses in Gulf countries face elevated risks due to their proximity to Iran and integration into global energy and trade networks. Free zones, trading hubs, and corporate structures in the Gulf have increasingly been targeted by illicit Iranian financial networks seeking to move funds, assets, and commodities under the veneer of legitimate commerce. Shell companies, trade-based schemes, shadow shipping, and offshore facilitation of high-risk flows illustrate how regional actors can be drawn into sanctions evasion networks or illicit financial activity more broadly. Additionally, the region faces heightened exposure to proliferation financing risks, as some of these illicit networks are known to channel funds toward Iran's military and dual-use programs, further amplifying legal and security exposures for regional businesses.

With the on businesses to operational, reputational, and regulatory risk, highlighting the importance of enhanced vigilance, strengthened AML/CTF controls, and cross-border cooperation with international enforcement partners in the current conflict environment.

The ongoing 2026 conflict is intensifying these challenges across all fronts. Escalating military activity and regional hostilities have increased the operational pressure on businesses and financial institutions, both within and outside the Gulf. Heightened geopolitical uncertainty drives rapid shifts in sanctions enforcement, disrupts trade and shipping routes, and increases scrutiny on cross-border financial flows. At the same time, illicit actors are likely adapting quickly, exploiting the volatility to expand shadow banking, trade-based schemes, and the use of charities or NPOs as conduits for funds.

For Gulf-based firms, proximity to conflict zones further elevates operational and security risks, while the threat of proliferation financing grows as networks exploit both legitimate-looking businesses and disrupted regional oversight to move resources toward Iran's military and dual-use programs. Collectively, these dynamics underscore that the ongoing conflict is not only a geopolitical crisis but also a catalyst for financial crime, sanctions evasion, and broader compliance exposure across the region.All organisations should be conductingenhanced due diligence on customers, suppliers, counterparties, intermediaries, and beneficial owners; continuous monitoring for indirect or multi-jurisdictional links to sanctioned entities, high-risk sectors, or opaque ownership structures; and — where relevant — comprehensive supply-chain due diligence to detect concealed trade-based schemes and other methods used to circumvent sanctions. Organisations should also remain alert to evolving tactics, including the use of front companies, complex corporate structures, and emerging digital channels such as cryptocurrencies or alternative payment systems.

These measures should be fully integrated into comprehensive compliance frameworks aligned with international standards and tailored to reflect the elevated, rapidly changing, and highly complex risks associated with Iranian financial activity. Ongoing monitoring, scenario planning, and proactive adjustments are essential to mitigate both regulatory and reputational exposure in this dynamic environment.

Financial Crime Risk Matrix

Crime Type	Risk Level*	Summary & Key Indices	Key High-Risk Sectors	Cross-Border Nexus
Money Laundering	High	Extremely high money laundering risk due to significant exposure to international financial and transnational crime, prevalence of informal financial networks, and lack of beneficial ownership or financial oversight. Iran remains on the FATF "high-risk jurisdictions subject to a call for action" list (often referred to as the blacklist), reflecting serious and ongoing strategic deficiencies in its AML/CFT and counter-proliferation financing frameworks. Global Organized Crime Index (see here)* Financial Crime: 10 / 9 AML Resilience: 10 / 2.5 *Global Organized Crime Index Score is on a 10-0 scale, with 0 denoting non-existent crime and 10 severe influence.	Trade-based sectors, finance, remittance & informal finance, energy & extractives, gold & precious metals, real estate, construction	Regional hawala networks, diaspora financial channels, smuggling networks, foreign-based shell companies
Sanctions & Export Control Evasion	High	Iran faces heavy international sanctions, including trade-restrictions, asset freezes, and travel bans. Currently the UN, US, EU, UK, France, Germany, Japan. Very-high risk of sanctions evasion via complex trade structures, front companies, and informal financial and corporate networks.	Banking, trade, transportation & supply-chain logistics, offshore finance, correspondent accounts	International trade-based evasion & smuggling, use of offshore companies and shell entities, regional hawala corridors (UAE, Türkiye, Iraq, Pakistan), and foreign-held assets or proxies in Europe, Asia, and the Gulf. High-Risk Jurisdictions: China, Hong Kong, Russia, Türkiye, Persian Gulf
Fraud	Medium-High	The Global Organized Crime Index found that cyber-fraud is widespread in Iran, including phishing attacks (e.g. fake text messages impersonating government services).	Banking & financial services, real estate, trade, public procurement	International fraud networks, international payment systems

Crime Type	Risk Level*	Key Indices	Key High-Risk Sectors	Cross-Border Nexus
Terrorist & Proliferation Financing	High	Extremely high terrorist and proliferation financing risks given exposure to regional terrorist financing networks and vulnerabilities in charitable foundations and cross-border remittance channels. The FATF continues to designate Iran as a jurisdiction of high concern for proliferation financing, urging enhanced due diligence and countermeasures by financial institutions. Global Terrorism Index (GTI) 2025 (see here)* Overall Score: 10 /6 (Ranked 18th of 163 countries) *The GTI scores each country on a scale from 0 to 10; where 0 represents no impact from terrorism and 10 represents the highest measurable impact of terrorism.	Charities & bonyads (quasi-state foundations), community fundraising, hawala, cash-based economy, trade-based activities	Regional hawala networks, diaspora channels, foreign-based intermediaries, use of trade routes for value transfer, correspondent banking gaps High risk jurisdictions: Lebanon (Hezbollah)
Bribery & Corruption	High	High corruption risk driven by opaque public procurement, weak oversight, discretionary regulatory authority, and entrenched bribery across public and private sectors. Transparency International Corruption Perceptions Index 2024 (see here)* 100/23 (Ranked 151st of 180 countries) *Transparency International Corruption Perceptions Index score is the perceived level of public corruption, where 0 means highly corrupt and 100 means very clean. Trace 2024 Bribery Risk Matrix (see here)* Rank: 185th ; Score 100/78 *Trace measures business bribery risk with a lower score indicating a lower bribery risk, while a higher score indicating a higher bribery risk. Global Organized Crime Index (see here)* Government Transparency and Accountability: 10 / 2 State-Embedded Criminality: 10 / 9.5 Private Sector Criminality: 10 /5 *Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence. Worldwide Governance Indicators (see here)* Control of Corruption: 10.38 *The WGI represent a country›s score and rank among all countries worldwide on each governance dimension.	Government contracting & procurement, state-owned enterprises, construction, trade, energy & extractives	Use of foreign intermediaries & front companies, trade-based corruption schemes, smuggling networks

Crime Type	Risk Level*	Key Indices	Key High-Risk Sectors	Cross-Border Nexus
Financial Secrecy	High	Medium financial secrecy risk stemming from opaque ownership and corporate structures, informal hawala networks and weak enforcement mechanisms.	Hawala, cash-heavy industries, company service providers, bonyads (quasi-state foundations), real estate	Use of offshore companies & nominee structures, foreign bank accounts, regional hawala networks, trade-based financial secrecy
Cybercrime	High	Cybercrime is widespread in Iran, involving both Iranian-based actors targeting domestic and foreign victims, and foreign-driven attacks directed at Iran. The ongoing conflict in 2026 has heightened this environment, with retaliatory cyber operations by Iran and Iran-aligned proxies increasing the frequency and sophistication of attacks. Limited cybersecurity enforcement and a heavy reliance on alternative digital channels due to sanctions further exacerbate the risks. **Read our Intelligence Briefing on Iranian Cyber Retaliation** (see here)*. Global Organized Crime Index (see here)* Cyber-Dependent Crimes: 10 / 8.5 *Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence.	Government and public sector, finance, trade & supply chains logistics	International hacking groups, offshore servers, cross-border malware campaigns targeting financial and commercial networks
Drug and Weapons Trafficking	High	Iran is both a production and transit country for the illegal drug trade. **Read our Drug Trade Dynamics in the Gulf report for information on Iranian specific threats** (see here)*. Global Organized Crime Index (see here)* Heroin Trade – 8.5 Cocaine Trade – 4.5 Cannabis Trade – 6 Synthetic Drug Trade – 9.5 Arms Trafficking – 9 *Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence.	Trade, supply chain logistics & transportation, financial services	Major transit country for opiates produced in neighbouring Afghanistan; synthetic drugs smuggling via trade routes (proximity to drug-producing regions) High-Risk Jurisdictions: Afghanistan, Pakistan, Türkiye, Persian Gulf

Crime Type	Risk Level*	Key Indices	Key High-Risk Sectors	Cross-Border Nexus
Modern Slavery & Human Trafficking	High	High risk of modern slavery and human trafficking, particularly forced labour, or sexual exploitation of refugees. Global Organized Crime Index (see here)* Human Trafficking – 8 Human Smuggling – 8.5 *Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence. US State Department's 2024 Trafficking in Persons Report Tier 3 – The Government of Iran does not fully meet the minimum standards for the elimination of trafficking and is not making significant efforts to do so.	Construction, agriculture, domestic labour, tourism	Trafficking networks in the Persian Gulf, refugee, and migrant flows
Environmental Crime	Medium-High	Global Organized Crime Index (see here)* Flora Crimes – 4.5 Fauna Crimes – 4 Non-Renewable Resource Crimes – 9.5 *Global Crime Index Score is on a 10-0 scale, with 0 being non-existent crime to 10 being severe influence.	Energy & extractions, gold & precious metals, logging & timber	International smuggling networks, transnational export control/ sanctions evasion networks
Tax Crime	Medium-High	Medium-high risk for tax crimes due to large informal economy (estimated historically at %45-30 of GDP), weak beneficial ownership transparency, and high levels of corruption.	Cash-based transactions, lawyers, accountants, real estate, company service providers, small-scale manufacturing, bonyads (quasi-state foundations)	Use of offshore companies & bank accounts, informal cross-border value transfer systems, smuggling routes

* Methodology: Each financial crime risk rating is derived from a combination of globally recognised indices and supplementary risk factors. Each index score is normalised and translated into a Red-Amber-Green (RAG) rating. Specifically, jurisdictions or entities are grouped based on their position within the distribution of index values, with the top, middle, and bottom third of scores per index corresponding respectively to Green, Amber, and Red (e.g. a 5/10 rating in one index would be equivalent to a 12/24 rating in another). Additional risk factors — such as enforcement actions, FATF evaluations, and our own Themis internal intelligence — also influence the final RAG classification through an overlay and adjustment process.

Regulatory Overview

Primary Anti-Financial Crime Regulators and Agencies:

- **Islamic Republic of Iran's Financial Intelligence Unit (IRFIU)** – Responsible for combating financial crime, the agency receives, analyses, and disseminates suspicious transaction reports on money laundering and terrorist financing under the Ministry of Economic Affairs and Finance.
- **Anti-Money Laundering High Council** – A cross-ministerial body led by the Minister of Economic Affairs and Finance that sets national AML/CFT policy and coordinates implementation.
- **Central Bank of Iran (CBI)** – Regulates and supervises financial institutions for AML/CFT compliance and enforces related violations.
- **Public Prosecution** – Investigates and prosecutes financial crimes and receives high-risk case files from the FIU.
- **Ministry of Intelligence** – Participates in AML/CFT investigations involving national security, including illicit finance and terrorist financing.
- **Law Enforcement Forces (including Cyber Police)** – Conduct investigations into money laundering, financial fraud, cyber-enabled financial crime and illicit financial flows.
- **General Inspection Organisation (GIO)** – Oversees public-sector integrity and investigates administrative and financial corruption within state institutions.
- **Supreme Audit Court (SAC)** – Audits public spending and detects financial irregularities and corruption within government entities.
- **General Headquarters for Combating Economic Corruption** – Coordinates national efforts against economic crimes, including corruption, embezzlement and financial misconduct.
- **Ministry of Economic Affairs and Finance (MEAF)** – Houses the FIU and leads national AML/CFT policymaking through its chairmanship of the High Council.
- **Ministry of Interior** – Works with law enforcement bodies to investigate financial crimes and participates in AML policymaking through the High Council.
- **Ministry of Commerce** – Oversees AML compliance in trade-related sectors and contributes to national AML/CFT coordination through its role on the High Council.

Key Anti-Financial Crime Legislation:

- **Anti-Money Laundering Law (2008, amended 2018):** Establishes the national framework for preventing and combating money laundering, including the creation of the FIU and the AML High Council.
- **Countering Financing of Terrorism (CFT) Law (2015, amended 2018):** Defines terrorist financing offenses and imposes requirements on financial institutions and government agencies to identify, report and prevent terrorist financing activities.
- **Executive By-laws of the AML Law (Multiple Regulations, last major update 2019):** Provide detailed procedures for customer due diligence, record-keeping, suspicious transaction reporting and supervisory enforcement.
- **Iran Penal Code (Islamic Penal Code – Economic Crimes Provisions):** Criminalises acts such as bribery, embezzlement, forgery and fraud, forming the basis for prosecution of financial and corruption-related offenses.
- **Law on Combating Goods and Currency Smuggling (2013, amended 2020):** Criminalises large-scale smuggling of goods and currency and introduces mechanisms to track illicit financial flows linked to smuggling networks.
- **Law on Transparency and Preventing Abuse of Government Resources (Anti-Corruption Framework):** Strengthens public-sector financial transparency and addresses corruption vulnerabilities within state institutions.
- **Foreign Exchange Regulations (Central Bank Directives):** Impose controls and reporting requirements on foreign currency transactions to prevent illicit financial flows and sanctions evasion.
- **Banking Anti-Money Laundering Regulations (CBI AML/CFT Directives):** Require banks and financial institutions to implement KYC, risk-based monitoring and reporting mechanisms aligned with national AML/CFT standards.

Financial Action Task Force Assessment

Iran has a long-standing history of scrutiny by the Financial Action Task Force (FATF) due to systemic deficiencies in its AML/CFT frameworks. The country first came under international review in the early 2000s and, over time, the FATF has repeatedly highlighted gaps in Iran's legal, regulatory and enforcement regimes. These have included insufficient criminalisation of terrorist financing and money laundering, weak financial intelligence capabilities, lack of transparency in beneficial ownership and limited cooperation with international counterparts. Despite some domestic initiatives to align with FATF standards, structural and political obstacles, including the prominent role of IRGC-linked entities in the economy, have hampered consistent compliance.

In June 2010, the FATF listed Iran as a "High Risk Jurisdiction Subject to a Call for Action" (referred to as a "blacklist" designation), which was reaffirmed multiple times in subsequent evaluations. The FATF has consistently cited Iran's failure to address key strategic deficiencies, particularly in the areas of terrorist financing and proliferation financing and noted that sanctions pressure has, in some cases, exacerbated reliance on informal and opaque financial channels. This status has meant that FATF members are encouraged to apply countermeasures when dealing with Iranian financial institutions and entities, reflecting heightened scrutiny and risk for cross-border transactions.

Efforts to engage with the FATF have been intermittent. Iran has, at times, passed domestic legislation aimed at strengthening AML/CFT compliance, including adopting measures to improve transparency in corporate structures and financial transactions. However, the FATF continues to assert that these measures are insufficiently implemented or enforced, leaving Iran on its "high-risk" list as of 2025. The ongoing designation underscores persistent vulnerabilities for multinational businesses and financial institutions, highlighting the need for enhanced due diligence, rigorous transaction monitoring and vigilance against involvement in illicit financial flows linked to Iran.

Being blacklisted by the FATF has significant implications both for entities seeking to do business with Iran and for Iran itself. For companies and financial institutions, engaging with Iranian entities carries significant heightened regulatory, legal and reputational risks, as they are expected to apply enhanced due diligence - or may even be legally prohibited from processing transactions or doing business in Iran or with Iranian entities. Banks and payment processors outside Iran often decline Iranian clients or scrutinise their transactions intensively, which can slow or block trade, complicate financing and increase compliance costs.

For Iran, the FATF blacklist reinforces its financial isolation, limiting access to the formal global banking system, discouraging foreign investment and pushing domestic and international transactions into

shadow-banking networks, informal channels and other opaque structures. This environment not only perpetuates money laundering, terrorist financing and proliferation financing risks but also constrains legitimate economic growth, increases costs for Iranian businesses and reinforces the country's reliance on alternative and higher-risk financial mechanisms to sustain trade and state revenue.

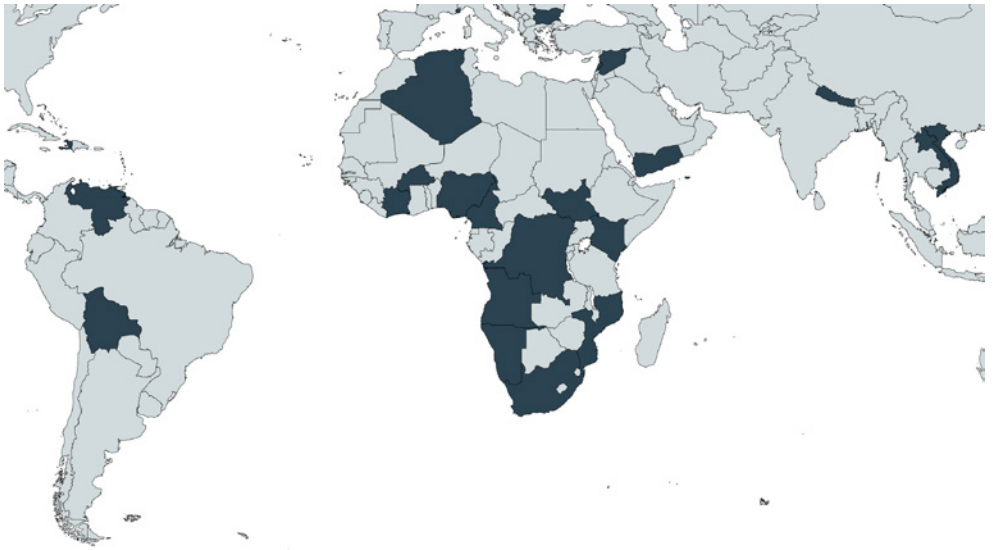
FATF 2026 Status

As of 2026, the FATF strongly encourages Iran to work with it to make further, urgent progress on its action plan to fully address:

- Adequately criminalising terrorist financing, including by removing the exemption for designated groups "attempting to end foreign occupation, colonialism and racism";
- Identifying and freezing terrorist assets in line with the relevant United Nations Security Council resolutions;
- Ensuring an adequate and enforceable customer due diligence regime;
- Demonstrating how authorities are identifying and sanctioning unlicensed money/value transfer service providers;
- Ratifying and implementing the Terrorist Financing Convention in line with the FATF standards, ensuring that the ratification and implementation of the Palermo Convention is also in line with the FATF standards, and clarifying the capability to provide mutual legal assistance; and
- Ensuring that financial institutions verify that wire transfers contain complete originator and beneficiary information.

Iran will remain on the FATF's black list until the full Action Plan has been completed. As the FATF previously stated, should Iran ratify and implement the Palermo and Terrorist Financing Conventions, in line with its standards, the FATF will decide on next steps - including whether to suspend countermeasures. The FATF may consider additional next steps if Iran fails to demonstrate further progress on its action plan.

FATF Grey Listed Countries as of June 2025



Sanctions Landscape

Iran has faced decades of international sanctions, driven by concerns over its nuclear program, alleged support for militant groups, and human rights record. Following the 1979 Iranian Revolution, the US imposed broad economic restrictions, including freezing assets and limiting trade. In the 1990s and 2000s, both the US and EU escalated sanctions targeting Iran's energy, financial, and shipping sectors, restricting oil exports, access to international banking, and foreign investment. The UN Security Council also imposed measures, including a 2006 arms embargo, restrictions on nuclear- and dual-use technology, and financial and energy sector limitations.

A major shift came in 2015 with the Joint Comprehensive Plan of Action (JCPOA), under which Iran agreed to curb its nuclear program in exchange for sanctions relief. The JCPOA was endorsed by UN Security Council Resolution 2231 in July 2015, which formally lifted certain UN sanctions in exchange for Iran's commitments to limit its nuclear program. Resolution 2231 provided a legal framework for monitoring Iran's nuclear activities through the IAEA, while suspending previous UNSC measures related to nuclear enrichment, arms transfers, and financial restrictions.
In 2018, the US withdrew from the JCPOA, reinstating broad sanctions on Iran's oil exports, banking networks, and shipping sector. These measures severely restricted Iran's access to global financial markets, disrupted critical trade flows, and sharply curtailed revenue from oil exports, which had long been a cornerstone of the national economy. The resulting economic pressure drove inflation to historic highs, caused a dramatic devaluation of the rial, and triggered a collapse in foreign investment, further exacerbating economic instability.

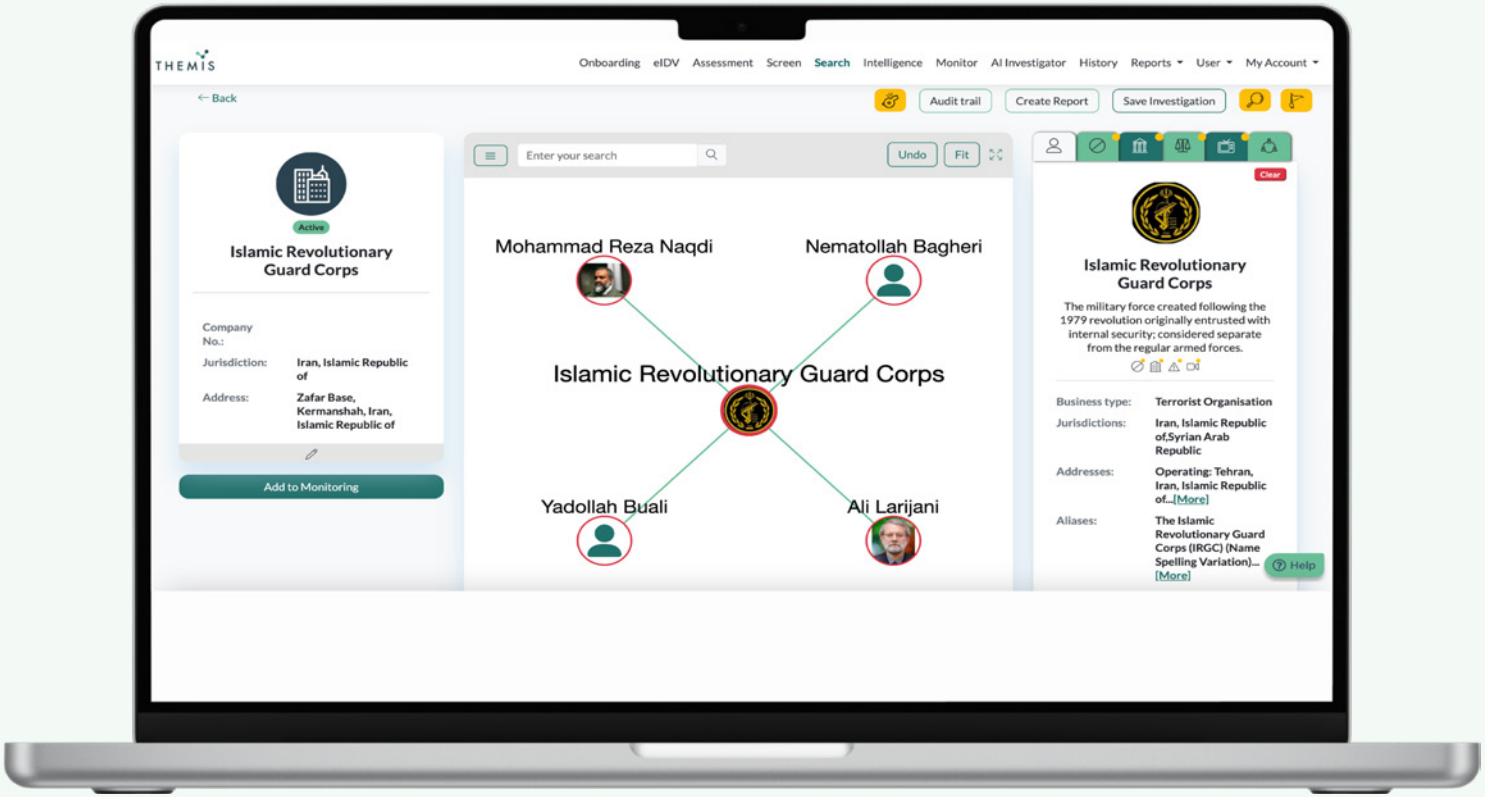
In 2025, France, Germany, and the UK triggered a "snapback" mechanism (a trigger to automatically reinstate sanctions if non-compliance with JCPOA was found). This led to the reinstatement of certain UN Security Council sanctions, including an arms embargo, restrictions on nuclear- and missile-related transfers, asset freezes and travel bans on designated individuals and entities, and limits on financial and trade activities connected to Iran's nuclear and missile programs. The EU and UK followed with complementary measures, restoring trade and financial restrictions aligned with UN mandates.

2026 Sanctions Landscape

In January 2026, the US imposed new sanctions targeting Iranian officials and entities in response to the government suppression of nationwide protests and to crack down on regime shadow-banking networks — part of an intensified "maximum pressure" campaign that has included designations under multiple executive orders. These actions freeze US-based assets and bar US persons from engaging with targeted individuals and entities. At the same time, G7 nations have also said that they are prepared to implement additional sanctions over the Iranian government's violent crackdown on protesters, indicating heightened multilateral resolve to escalate pressure if abuses continue.

In February 2026, the US further intensified its sanctions campaign against Iran with a new round of designations targeting the country's shadow fleet of oil tankers and ballistic missile programme. This reflects the increasing use of highly targeted sanctions aimed at disrupting Iran's illicit financial and trade networks.

The impact of ongoing geopolitical tensions and military escalation on sanctions remains uncertain, with the potential for the US to respond with additional measures. For businesses, these developments underscore a rapidly evolving and high-risk environment. The renewed US actions, coupled with potential new G7 sanctions, highlight that authorities are willing to move quickly and multilaterally when deemed necessary. Companies operating in markets connected to Iran, or engaging with counterparties in high-risk sectors such as oil, shipping, logistics, or finance, must maintain rigorous compliance frameworks, closely monitor sanctions updates across all jurisdictions, and apply heightened due diligence to avoid inadvertent exposure. Even routine commercial transactions now carry elevated risk, making proactive risk assessment and conservative engagement essential in 2026.



Threat Spotlight

Corporate Concealment: The risk of Iranian linked companies dressed up in a GCC country's national dress

Sanctions Circumvention Through Company Formation and Trade Structuring

In today's interconnected global markets, there is a significant risk of inadvertently engaging with companies that are looking to circumvent sanctions — not only in high-risk sectors like energy and logistics, but also in sectors traditionally considered lower risk such as marketing or social media companies. In the case of Iran, prolonged sanctions have led some Iranian entities and individuals to develop increasingly sophisticated methods to sustain access to global markets and supply chains, leaving well-intentioned companies and individuals vulnerable to inadvertent compliance risks.

A central tactic used by evasion networks is the creation, acquisition or repurposing of companies abroad, often in well respected international financial centres, or jurisdictions with high trade volumes, complex corporate-registration systems or limited visibility into beneficial ownership. These firms frequently look legitimate and present as credible commercial partners, often using local country nationals and intermediaries who are appointed both on official registries as the named company director(s) as well as publically acting as the CEO or leadership team. This obscures the true leadership andbeneficiaries of the new entity and presents it as a legitimate local entity with no obvious links back to Iran. Beneath the surface, however, the real Iranian owners use these front companies to avoid sanctions, load the company with debt, buy assets and high value goods, facilitate business and financial transactions or help to move restricted goods into or out of Iran.

Common patterns include the establishment of companies in regional trade and financial hubs across the GCC, as well as offshore corporate hubs in the Caribbean, Europe, North America, and Asia. These entities may operate directly or through multiple layers of intermediaries designed to obscure any ties with Iran. They often appear active across routine sectors but ones with ties to sanctioned materials or companies — logistics, commodities, machinery, pharmaceuticals, engineering, and even dual-use technology — making them difficult to distinguish from legitimate market players.

Circumvention schemes frequently rely on complex trade structures, including transshipment, re-labelling, and diversion routes in which goods are legally exported to an intermediary country before being re-exported to Iran. To further distance themselves from scrutiny, front companies may appoint foreign directors, use nominee shareholders, or engage professional corporate-services firms that mask true beneficial ownership.

Many of these entities are designed to blend seamlessly into normal commercial activity. At first glance, they can look like reliable trading partners. Only deeper, targeted due diligence, focused on ownership, trade patterns, counterparties, and the economic rationale of transactions, reveals the hidden links to sanctioned actors. Understanding these risks is essential for companies aiming to protect themselves from regulatory exposure, financial loss, and reputational harm.

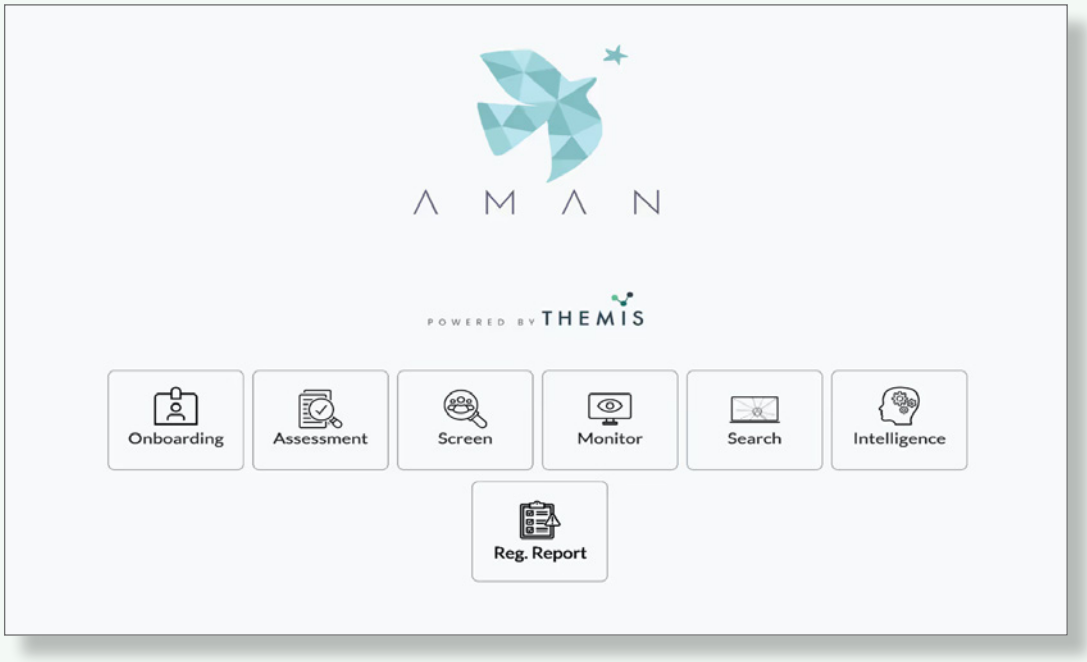
The practice of corporate concealment presents a significant set of legal, regulatory, financial and reputational risks to companies that then trade with these front companies. Given the widespread nature of this activity from Iran and Iranian actors, it can also cause significant reputational damage at a national level, undermining the 'host' country's reputation for trust, transparency and good corporate governance.

Bahrain: A Case for Proactive Measures Against Corporate Concealment

Bahrain has taken a coordinated approach to addressing corporate concealment and sanctions circumvention risks, signalling what effective and proactive risk mitigation can achieve. The Kingdom has brought the public and private sectors together to enhance oversight of and due diligence on complex corporate structures.

Central to this effort is AMAN, the national anti-financial crime platform, which allows authorities and businesses to map ownership structures, identify hidden network connections, and detect potential links to sanctioned individuals or entities. By providing a clearer view of corporate networks, the platform supports earlier detection of suspicious activity and more informed decision-making.

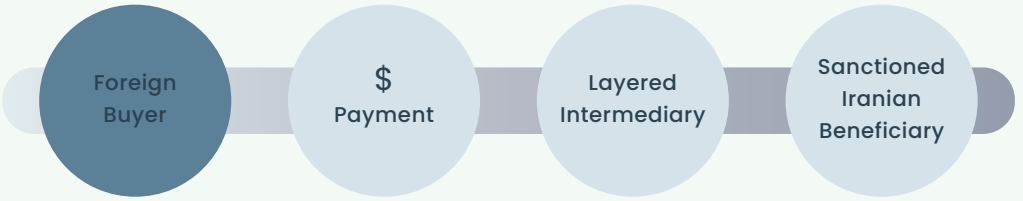
AMAN also facilitates information sharing between public and private sector stakeholders, enabling regulators, financial institutions, and corporate actors to respond to emerging risks collectively. This approach helps reduce the likelihood that sanctioned actors can establish entities within Bahrain, limiting the flow of dirty money through the Kingdom.



The Sanctions Evasion Playbook

What would an Iranian-linked front network look like? This scenario illustrates how a sanctions-designated Iranian exporter might attempt to obscure the flow of funds from an overseas oil sale by using layered intermediaries and opaque corporate structures.

* This scenario is hypothetical and provided for illustrative purposes only; it does not reflect an actual entity, transaction, or investigation.



Steps:

1. Establishing Overseas Front Companies

A sanctions-designated Iranian exporter typically begins by forming front companies in jurisdictions that provide corporate opacity. These firms are incorporated through local service providers who can supply nominee directors, minimal disclosure requirements and legitimate-looking business licenses. To appear credible, the companies may create basic websites, social media pages or trade documentation. Often, several entities are established at once to create redundancy and make the network appear like a diversified trading group.

2. Creating Commercial Documentation to Mask the Oil Transaction

Before any funds move, the network constructs documentation that disguises the underlying oil trade. This may include re-invoicing the transaction as a sale of generic commodities or industrial materials unrelated to petroleum. Shipping paperwork can be routed through multiple ports or rely on ship-to-ship transfers to further obscure the cargo's origin. Contracts may be short-term, vague or governed by third-country legal frameworks to prevent easy scrutiny. The overall goal is to generate a plausible commercial narrative that conceals the sanctioned trade.

3. Moving Funds into the Front Company

The overseas buyer is instructed to pay the front company rather than the Iranian exporter, enabling the proceeds to enter the financial system under a different identity. Payments may be split into smaller sums or sent through several intermediary banks to reduce the likelihood of sanctions screening alerts. These transfers are often made in non-USD currencies and justified with ambiguous commercial descriptions. In some cases, funds move through additional shell entities or payment providers in low-risk jurisdictions to add extra layers of concealment.

4. Repatriating Funds to Iran

Once the funds reach the front company's account, the network must return the value to Iran without using restricted banking channels. This is usually done through informal value-transfer systems, such as hawala networks or trusted regional exchange houses that settle balances through off-ledger accounting. Proxy agents may physically move cash or redirect payments to third parties who can complete settlements on behalf of Iranian beneficiaries. Sometimes, funds are repatriated indirectly by overpricing imported goods, embedding the profit margin in commercial shipments rather than in visible financial transfers.

Implications for Businesses: Due Diligence, Network Mapping and Technology

For businesses, networks like these highlight the critical importance of thorough due diligence and sanctions screening at every stage of a transaction. It is not enough to simply vet the immediate counterparty; companies must also understand the **ownership structures, affiliations, and past histories of any intermediaries, agents or front companies** involved. Network mapping and screening, including analysing the relationships between entities, directors and geographic locations, becomes essential to identify hidden connections that could expose a business to sanctions risk.

Automated tools, AI-driven analytics and cross-border data sources allow compliance teams to detect these opaque links more efficiently, uncover suspicious patterns and assess the risk of indirect exposure. By investing in these capabilities, companies can avoid inadvertently doing business with entities that serve as fronts or proxies, strengthen their compliance posture and maintain regulatory trust while conducting legitimate international trade.

Key Red Flags to Spot Corporate Concealment and Potential Sanctions Circumvention

Even the most legitimate seeming company can be masking connections to sanctioned entitles or actors. Warning signs rarely appear in isolation and normally require looking across multiple degrees of separation. This is why it is so important for all organisations to do not just surface level due diligence, but DD on multiple layers of separation. Spotting various potential red flags — like a company in a permissive jurisdiction using layers of nominees and operating in a higher risk sector such as oil — should trigger deeper scrutiny. Some red flags to watch out for include:

Ownership That Feels Confusing Establishing Overseas Front Companies

- Companies with layers of owners or intermediary firms in secrecy-friendly jurisdictions, making it difficult to identify who ultimately controls the entity.
- Directors or shareholders who only exist on paper — individuals with no digital footprint, no industry history or whose LinkedIn profiles appear hastily created or unusually vague.
- Leadership that rotates suspiciously often, with directors or shareholders changing every few months without any operational explanation.
- Firms that suddenly shift ownership across borders, especially into jurisdictions commonly used as "waypoints" for Iranian-front structures, with no clear commercial logic.
- Beneficial owners who appear linked to multiple unrelated companies, sometimes spanning sectors that have no business interacting — a hallmark of corporate structures designed for concealment rather than commerce.
- Companies that claim "local ownership" but operate entirely from abroad, or whose supposed owners have no visible presence in the country where the company is registered.

Trade Patterns That Make Little Commercial Sense

- Frequent re-labelling, re-packaging or repackaging of dual-use goods or goods in sanctioned sectors, often with inconsistent documentation.
- Trade routes that look like detours, not supply chains — shipments that zigzag through multiple intermediary countries with no commercial logic, often adding time and cost with no clear benefit.
- Unusual spikes or drops in export volumes to certain jurisdictions known for re-exporting to Iran, particularly when the shifts coincide with enforcement actions or new sanctions designations.
- Intermediaries with no clear value-add — trading companies inserted between suppliers and buyers whose role is unclear, except perhaps to add distance from the original source.
- Goods declared under vague or overly broad customs categories, such as "machinery parts" or "industrial equipment," making it difficult to verify the actual nature of the shipment.
- Mismatch between the company's profile and its trading behaviour — for example, a small office-based consultancy suddenly shipping heavy industrial machinery, medical equipment or controlled electronics.
- Repeated use of free-trade zones or ports known for transshipment without a credible operational explanation, especially when the goods do not require value-added services provided in those zones.

A Lack of Transparency

- Companies that avoid answering basic questions about ownership, suppliers or operations, or respond with vague, formulaic statements that don't address the specifics asked.
- Minimal online footprint or inconsistent registration details, including conflicting addresses, missing corporate filings or websites with generic or placeholder content.
- Overreliance on intermediaries, lawyers or "corporate service providers" who insist on communicating on the company's behalf, even for routine commercial inquiries.
- Limited or no traceable track record, including no visible customers, partners or verifiable transaction history, despite claims of years in business.

Companies Operating in High-Risk Sectors in Unusual Ways

- Companies that market themselves as a general trading firm or "multi-sector distributor" when involved in higher-risk commodities, including machinery, pharmaceuticals, petrochemicals or dual-use technology.
- Activities that appear routine on the surface but rely on unnecessarily complex contracts or frequent cross-border business that makes little commercial sense.
- Companies that shift industry focus abruptly, such as a textile trader suddenly brokering industrial chemicals or precision electronics.
- Firms dealing in "grey zone" goods – items not explicitly controlled or sanctioned but known to be prized in Iran's trading networks (e.g. high-spec machine parts).
- Unusual interest in items with known re-export risks, like automotive components or telecommunication hardware, especially when the company operates in a country commonly used as a transshipment hub.
- Companies that offer "end-to-end" services they cannot realistically support, such as logistics firms promising procurement, financing, customs clearance and technical certification, despite minimal staff or facilities.
- Sector activity that spikes following new sanctions, suggesting the company may be filling gaps created when established distributors halt trade.

Jurisdictional Elements That Raise Eyebrows

- Operations routed through countries repeatedly cited in sanctions-circumvention cases, especially those serving as re-export hubs for Iran-bound goods.
- A footprint concentrated in jurisdictions with high trade flows but weak enforcement, where companies can easily blend into dense commercial ecosystems.
- Shipping routes that consistently pass through the same permissive ports or free-trade zones, even when these add cost or time with no operational justification.
- Entities registered far from where they actually conduct business, such as companies incorporated in one region but trading almost exclusively in another known for sanctions risk.
- A cluster of related companies sharing the same addresses, agents, or service providers in jurisdictions where Iranian-controlled networks have historically operated.
- Frequent shifts of corporate domicile, with the company relocating from one permissive jurisdiction to another within short timeframes — a tactic often used to stay ahead of regulators.
- Transactional links that trace back to regions with established Iranian diaspora commercial networks, particularly where past circumvention cases have involved community-based intermediaries.

Case Study

Iranian Shadow Banking Operations

The US government agency, FinCEN, published a Financial Trend Analysis in late 2025 examining an alleged Iranian shadow banking network. Drawing on reports from US financial institutions, FinCEN identified roughly $9 billion in financial activity during 2024 linked to potential Iranian shadow banking operations. According to the analysis, these networks span multiple continents, with key intermediaries based in countries such as Hong Kong, the UAE and the UK. Intermediaries used in these countries operate through a complex web of Iranian front companies — including oil firms, shell entities, shipping and investment companies, and technology procurement firms — that collectively transact billions of dollars across the globe annually.

These shadow networks are comprised of different types of intermediaries which are used for a range of purposes, including:

- Foreign oil and shipping companies which appear to be Iranian front companies moving billions in illicit oil sales.
- Foreign investment companies that are used to provide access for Iranian actors to international investment markets.
- Shell companies facilitating Iranian procurement of export-controlled technology and dual-use goods.
- Shell companies that receive shadow banking funds and move funds to other jurisdictions.
- Intermediaries with access to US and European financial institutions.

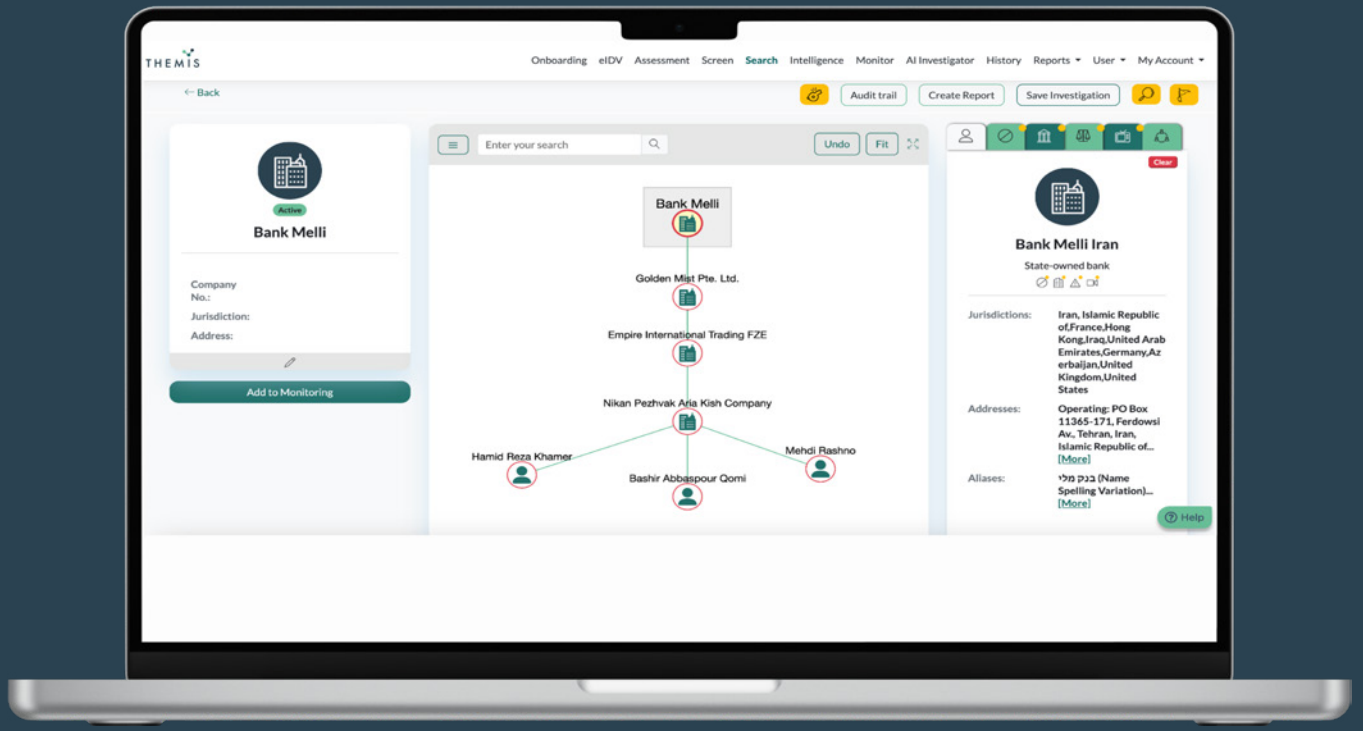
Multinational businesses and financial services have been inadvertently implicated as counterparties in these networks, unknowingly facilitating illicit financial flows for Iranian actors. This underscores how companies can be exposed to risks associated with Iranian financial crime, even if they are not conducting business directly with Iranian entities or the Iranian government, and even when their intention is purely above board.

FinCEN identified several distinct networks within this alleged Iranian shadow banking system. One involved dozens of foreign oil companies, primarily in the UAE and Singapore, that collectively sent or received approximately $4 billion linked to Iranian oil firms – without the knowledge of local regulators or law enforcement. Another network of shell companies routed about $5 billion through Hong Kong and the UAE. A third network comprised investment firms in the UK and Switzerland that were engaged in transactions worth hundreds of millions of dollars, again without the knowledge of local authorities. The analysis further noted that US correspondent bank accounts were also used in connection with these activities.

Expanding on this, in early 2026 the US imposed sanctions on additional actors within Iran's shadow banking system. The measures targeted what are referred to as "rahbar" companies — intermediary entities established by Iranian banks to manage the international transactions of their clients. These companies operate in close coordination with Iran-based clients to facilitate cross-border trade payments, relying on a complex network of front companies and exchange houses across multiple jurisdictions. Through these networks, sanctioned actors can obscure the origin and destination of funds, layer transactions across jurisdictions, and effectively launder revenue, allowing the Iranian regime to sustain critical financial flows that would otherwise be blocked by international sanctions.

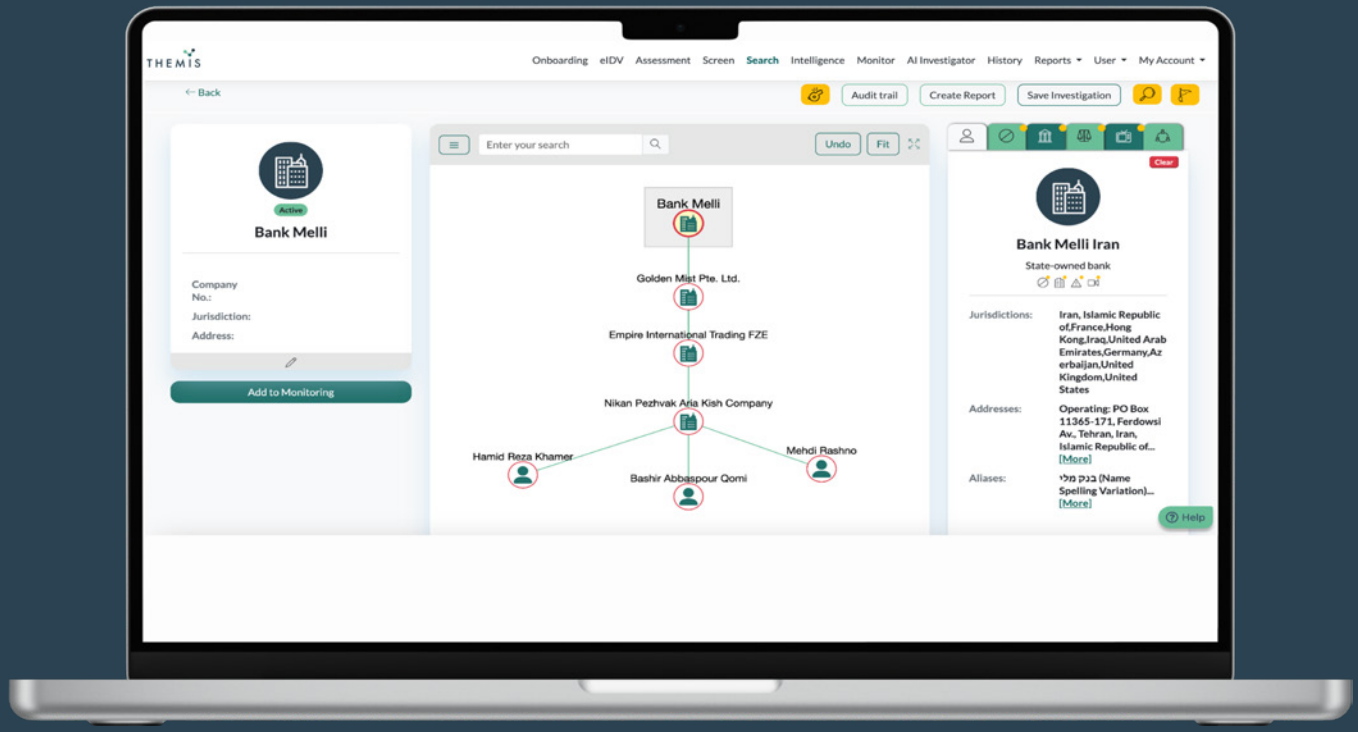
BANK MELLI's MONEY LAUNDERING NETWORK

According to the OFAC, Bank Melli has created an extensive network of cover companies to send and receive funds outside of Iran. Per OFAC, Iran-based Nikan Pezhvak Aria Kish Company is the head of Bank Melli's rahbar network in Iran and UAE-based Empire International Trading FZE is Bank Melli's foreign-based rahbar company used for managing foreign currency. Empire International has also reportedly provided customers with details of cover companies, enabling millions of dollars in foreign currency revenue.



BANK SHAHR MONEY LAUNDERING NETWORK

According to OFAC, the UAE-based HMS Trading FZE serves as a commercial front company on behalf of Shahr Bank as a key element in Iran's oil export and rahbar shadow banking mechanism. HMS Trading and Iran-based Tejarat Hermes Energy Qeshm are reportedly responsible for overseeing the commercial trade activities of Shar Bank's rahbar network via numerous front companies. OFAC alleges that HMS Trading relies on a number of financial front companies in both the UAE and UK.



Why This Case Matters: The FinCEN report highlights how Iranian shadow banking networks can reportedly move billions of dollars globally while obscuring ultimate beneficiaries, often linked to sanctioned goods such as oil. Even companies with no direct dealings with Iranian oil may become inadvertently involved in these illicit flows, exposing them to regulatory, reputational and legal risks. Understanding these networks is critical for financial institutions and multinational businesses to strengthen due diligence, mitigate sanctions exposure and prevent unintentional facilitation of illicit activity. The global scale of these operations underscores the importance of cross-border cooperation and vigilance in monitoring complex financial networks.

KEY TAKEAWAYS:

- **Enhanced Due Diligence:** Strengthen due diligence and screening for all counterparties and network connections in high-risk sectors or jurisdictions associated with Iranian sanction evasion, even when transactions, investments or business deals appear legitimate.
- **Corporate Structure Monitoring:** Closely monitor complex corporate entities to uncover potential front companies that obscure beneficial ownership, end-users or supply chain participants — particularly in oil, shipping, investment and technology procurement sectors.
- **Risk of Financial Intermediaries:** Recognise that US correspondent banks and global financial intermediaries may be exploited, potentially exposing businesses to regulatory violations. Implement robust compliance policies and tools to prevent inadvertent involvement.
- **Cross-Border Information Sharing:** Develop protocols for sharing information across jurisdictions to detect, manage and mitigate exposure to Iranian multi-jurisdictional financial crime networks.

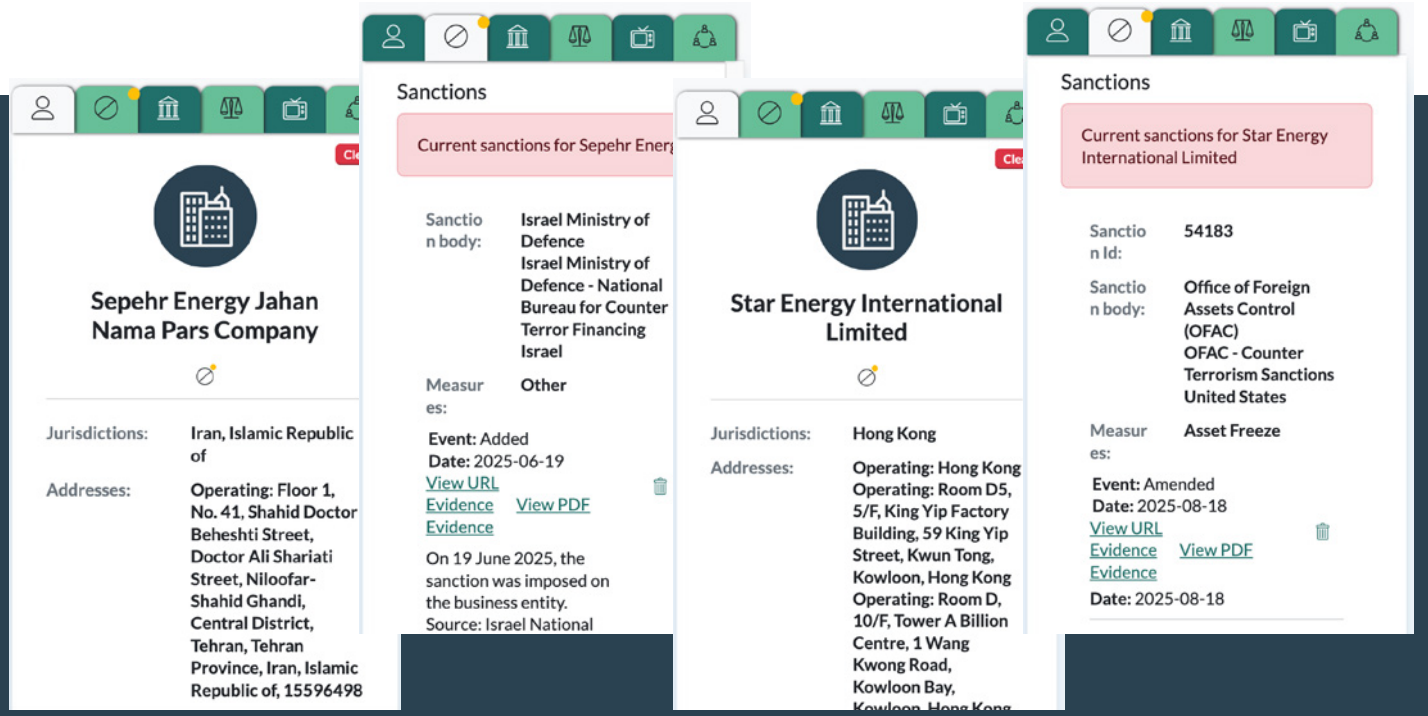
Case Study

Iranian Chinese Oil Smuggling Networks

In 2025, The US Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on nearly two dozen firms allegedly tied to Iran's oil trade, accusing them of helping Iran covertly export oil to China and then using those revenues to fund its military and terrorist activities. The potential circumvention of trade restrictions on Iranian oil by China has become a central concern for international authorities. Although China has officially reported no imports of Iranian oil since 2022, experts believe that illicit Iranian and Chinese actors have collaborated to covertly move billions of dollars' worth of Iranian crude into the country. One report estimated that China bought 80% of shipped Iranian oil in 2025, to put this into perspective.

According to the US Treasury, Iran's Armed Forces General Staff (AFGS) and its main commercial affiliate, Sepehr Energy, continue to establish front companies and rely on buyers and facilitators to enable the trade of sanctioned oil. Sepehr reportedly carries out oil shipments through a series of "deals" between multiple front companies, creating an elaborate system of oil smuggling and money laundering. Many of these front companies are based in China and Hong Kong - such as one company called Star Energy, which has moved tens of millions of dollars on behalf of Sepehr Energy.

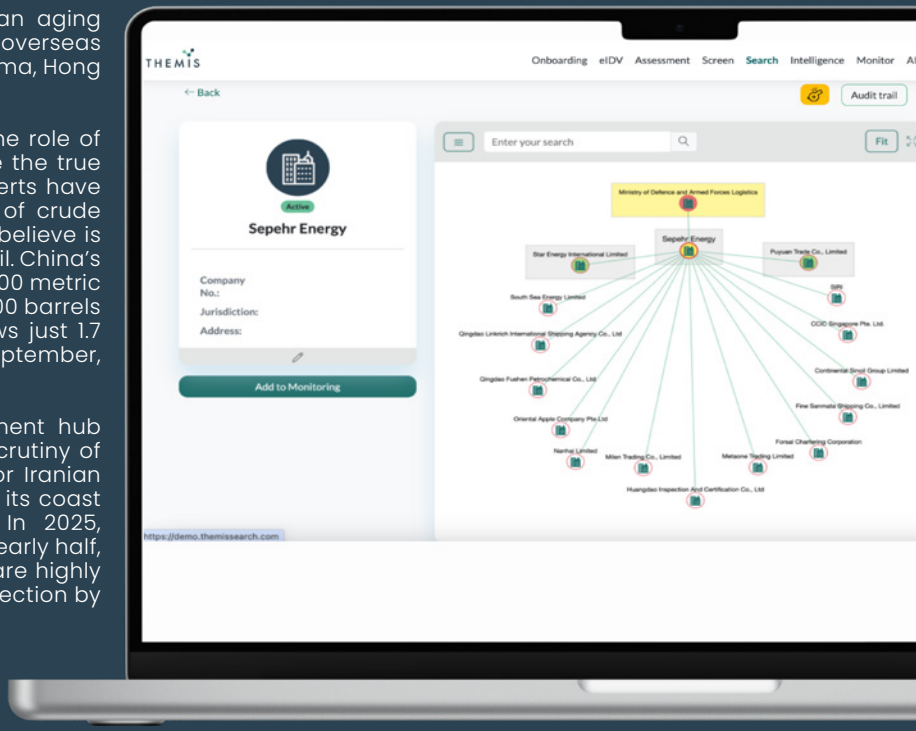
Trade-Based Smuggling Mechanisms: One case perfectly illustrates how Iranian oil is covertly moved into China - and the many front companies involved. From mid-2023 to mid-2024, Hong Kong–based Puyuan Trade Co. delivered multiple shipments of Iranian crude oil to Sepehr Energy front Xin Rui Ji at Qingdao Port in Shandong Province. To evade detection, the oil's origin was concealed through ship-to-ship transfers and falsified documentation, aided by transportation and inspection firms — including a Singapore-based company that certified the cargo as non-Iranian. Once the disguised oil reached China, Sepehr depended on cooperative local port agencies in Shandong - home to numerous independent "teapot" refineries that regularly purchase Iranian crude oil and manage the movement and storage of these illicit shipments.



Authorities allege that Iran relies on access to an aging "shadow fleet" of oil tankers for its shipments of oil to overseas buyers, including ships flagged in Cameroon, Panama, Hong Kong and the Seychelles.

A reported key component of these networks is the role of trade from other countries being used to obscure the true origin of the Iranian sourced oil. For instance, experts have pointed to a surge in unusually large quantities of crude oil from Indonesia to China - a trend that traders believe is linked to masked shipments of sanctioned Iranian oil. China's oil imports from Indonesia rose from less than 100,000 metric tons in 2024 to 9.81 million tons in 2025 - over 235,000 barrels per day. However, Indonesian customs data shows just 1.7 million tons of crude exported from January to September, with only 25,000 tons going to China.

This reported shift to Indonesia as a transshipment hub for Iranian oil to China comes after widespread scrutiny of Malaysia's role as a major trans-shipment hub for Iranian oil - including reports of ship-to-ship transfers off its coast and significant discrepancies in import data. In 2025, China's reported oil imports from Malaysia fell by nearly half, suggesting that Iranian trans-shipment networks are highly adaptive and are rerouting shipments to avoid detection by authorities.



Case Study

Iranian Links to Regional Captagon Trade

Over the past decade, the Captagon trade has emerged as one of the Middle East's most lucrative illicit drug markets. Driven by a vast underground production industry and intricate smuggling networks often linked to regional state-affiliated actors or militia groups, the trade poses a significant regional criminal threat. Captagon generates substantial revenue, much of which is believed to fuel regional conflict and fund extremist networks.

While Syria was historically the primary source of Captagon production, the dismantling of the Assad regime and subsequent efforts by the new Syrian government to crack down on domestic manufacturing have created opportunities for production sites and trafficking routes to emerge elsewhere in the region. This shift has heightened vulnerabilities for regional countries, exposing them to new risks associated with Captagon flows and complicating law enforcement efforts.

One particular concern is the growing role of Houthi-controlled areas in Yemen in the production and trafficking of Captagon. In June of 2025, Yemeni authorities seized 1.5 million Captagon pills — valued at an estimated $21 million wholesale and up to $30 million retail — hidden in a truck traveling from Houthi-held territories to Saudi Arabia. Officials noted that the bust reflects the presence of extensive production and smuggling networks within Houthi areas.

Yemeni authorities have indicated that they believe the Iranian regime is acting as the principal financier and coordinator behind these Houthi-linked operations. Iran is reportedly involved in establishing production facilities, providing logistical support and facilitating regional trafficking networks, effectively integrating Captagon production and smuggling into its broader regional influence strategy and illicit finance networks.

Why This Case Matters: The evolution of Iran's role in Captagon production and trafficking highlights the adaptability and resilience of Iranian-linked illicit financial and criminal networks. This case shows how these networks are quick to pivot to new mechanisms — such as the Captagon trade — to generate new revenue, fund proxy groups and extend their regional leverage. This underscores that illicit networks are not static; they can exploit geopolitical dynamics and new illicit opportunities, directly affecting regional stability, trade and investment environments.

KEY TAKEAWAYS:

- Iranian-linked illicit financial and criminal networks demonstrate high adaptability, using illicit trades like Captagon to fund proxies and expand influence.
- New trafficking routes and production hubs increase the risk of indirect exposure for companies involved in logistics, trade and finance.
- Vigilance in monitoring evolving criminal networks and regional enforcement actions is critical for mitigating operational risk.
- Businesses should integrate geopolitical awareness into compliance and risk management strategies to navigate these complex dynamics.

Case Study

Forced Labour of Children in Iran

Iranian and Afghan children experiencing homelessness in Iran are highly vulnerable to forced labour, with experts finding that child trafficking in the country has increased in recent years. According to the US 2024 Trafficking in Persons report on Iran, experts believe there are approximately seven million children who are sold or rented to work in the country, mostly between the ages of 10 and 15 years old. A majority of these children are undocumented foreigners - most notably, Afghan refugees. These children are forced to work in a range of low-skilled industries, including textiles, manufacturing, agriculture, construction, transport and waste disposal. Many children are also forced into domestic servitude or sex work.

Media and international authorities have reported an increase in the number of overall child labourers in Iran, particularly "scavenger children", who work and live in and on garbage dumps. Undocumented and unaccompanied Afghan children from Herat (a city close to the Iranian-Afghanistan border) are highly vulnerable to trafficking and reportedly make up a majority of these "scavenger children". Criminal groups also reportedly kidnap Iranian and migrant children to work as beggars and street vendors in cities, as well as forcing them to engage in crimes such as drug trafficking and smuggling. There are also reports of coercion of children into armed groups in the region.

Importance of Supply Chain Due Diligence: Given this context, any company seeking to engage with Iranian counterparts, especially in sectors known for high child labour risk, should screen for potential red flags linked to human trafficking or forced labour. Enhanced due diligence is particularly critical in industries such as textiles, agriculture, waste management, construction and domestic services, where child labour has been documented extensively throughout the country.

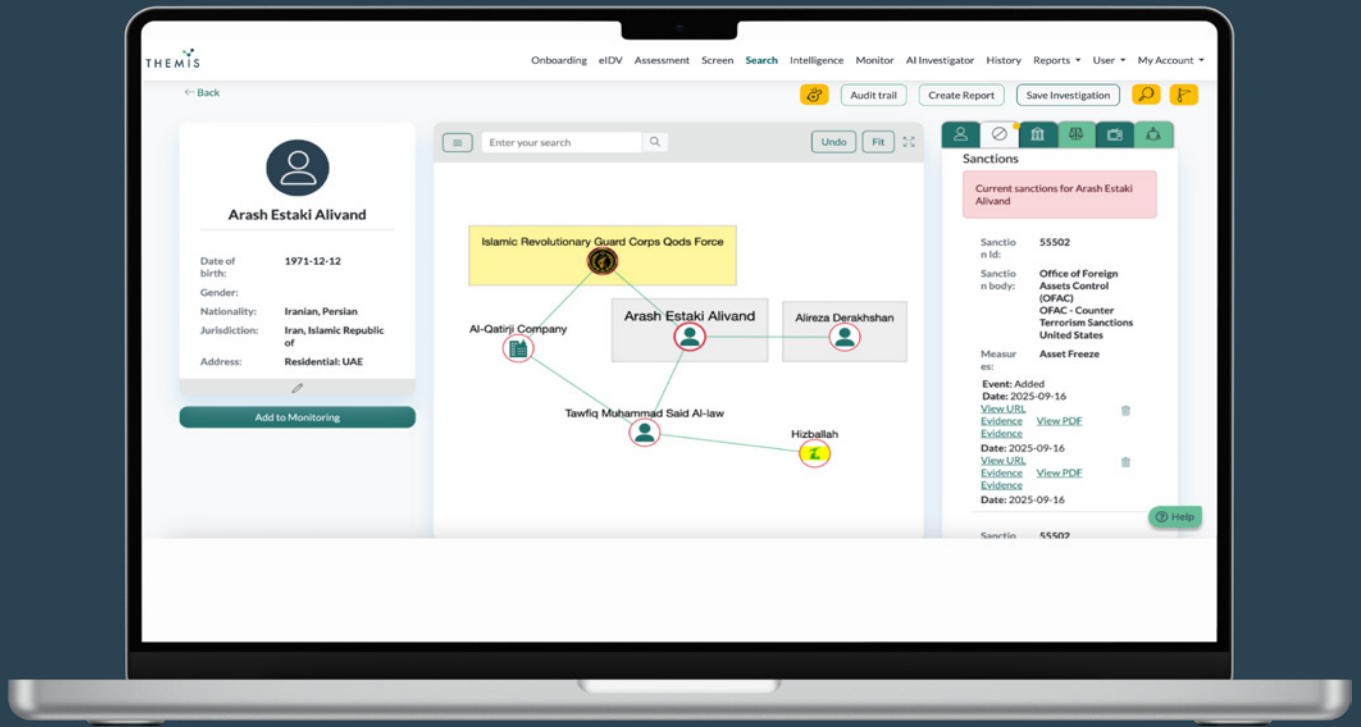
Companies must not assume that partners or suppliers are compliant. Businesses have a responsibility to conduct robust due diligence processes, including verifying the sources of their supply chains, auditing subcontractors, and ensuring compliance with international child protection and modern slavery standards. Failure to take these steps could not only contribute to human rights abuses but also expose companies to significant legal, financial and reputational risks.
purchase Iranian crude oil and manage the movement and storage of these illicit shipments.

Case Study

Use of Cryptocurrency by IRGC Proxy Networks

In 2025, US authorities designated a pair of Iranian financial facilitators and over a dozen Hong Kong and UAE based individuals and entities for their alleged role in coordinating cryptocurrency transactions on behalf of the IRGC and other Iranian defence actors. The two Iranian nationals, Alireza Derakhshan and Arash Estaki Alivand, coordinated the purchase of over $100 million worth of cryptocurrency for the Iranian government from 2023 to 2025. They used their network of foreign front companies to transfer the cryptocurrency funds to Iran.

Moreover, Alivand has worked as a financial facilitator and oil broker for the Syria-based Al-Qatirji Company, which has served as a primary partner of the IRGC-QF (the IRGC's external operations force) in the sale of Iranian oil. Alivand was also involved in transactions worth millions of dollars with Tawfiq Muhammad Sa'id al-Law, a Hezbollah-associated money changer who provided Hezbollah with access to digital wallets in order to receive funds related to IRGC-QF commodity sales, and who conducted cryptocurrency transfers on behalf of the Al-Qatirji Company.



Areas of Financial Crime Vulnerability

- **Extensive sanctions pressure driving illicit financial channels:** Long-standing international sanctions have pushed some actors and entities in Iran to develop alternative financial networks, which, by design, operate with opacity and create systemic exposure to sanctions evasion, money laundering, terrorist financing and fraud. While these channels allow these Iranian actors to maintain some access to international economic and trade activity, they inherently operate with low transparency and high-risk of misuse and illegality. Such networks are frequently exploited for laundering illicit proceeds, funding sanctioned entities, and facilitating fraud.

- **Large informal and cash-based economy:** Iran's economy relies heavily on cash transactions, unregistered businesses and hawala-style money-transfer systems, as well as international remittance and value-transfer networks, which allow financial flows to move outside the formal banking sector. This environment makes it difficult for authorities to identify and prevent illicit financial flows. The combination of widespread informal finance and weak reporting requirements significantly heightens the risk of money laundering, tax evasion and terrorist financing.

- **Weak regulatory oversight and fragmented supervision:** Iran's AML/CTF regulatory framework is hindered by overlapping responsibilities among multiple agencies, inconsistent enforcement of laws and gaps in financial supervision. Beneficial ownership information is limited or difficult to access, reducing transparency and enabling individuals and entities to hide illicit activities. Agencies such as the Central Bank, Ministry of Finance and the FIU have regulatory authority but face resource constraints and lack full independence, which can delay or weaken investigations. This fragmented structure creates systemic vulnerabilities that criminal actors can exploit across both domestic and cross-border financial transactions.

- **Dominance of state-owned enterprises (SOEs) and bonyads (quasi-state foundations):** Large SOEs and bonyads control key sectors of the Iranian economy, including energy, construction and import-export operations. These entities often enjoy political protection and operate with limited external oversight, weak auditing processes and minimal transparency. Such conditions can facilitate corrupt practices, including sanction evasion, embezzlement, bribery, and financial mismanagement. Moreover, because these organisations control substantial assets and resources, corruption or misuse within them can have wide-ranging economic and social effects, such as recent economic instability in the country.

- **High-risk cross-border corridors and geopolitical positioning:** Iran's geographic location — bordering Afghanistan, Pakistan, Iraq and Türkiye — places it at the centre of multiple high-risk smuggling and trafficking routes. These corridors are used for narcotics, weapons, human trafficking and other contraband, all of which intersect with illicit financial networks and transnational organised crime. Moreover, smuggling routes are also often linked

to sanction or export control evasion, as well as potentially terrorist and proliferation financing. Porous borders, combined with weak enforcement in remote areas, allow criminal organisations to integrate illicit proceeds into both domestic and international financial channels. Geopolitical tensions and regional instability further complicate law enforcement and create persistent avenues for illicit finance.

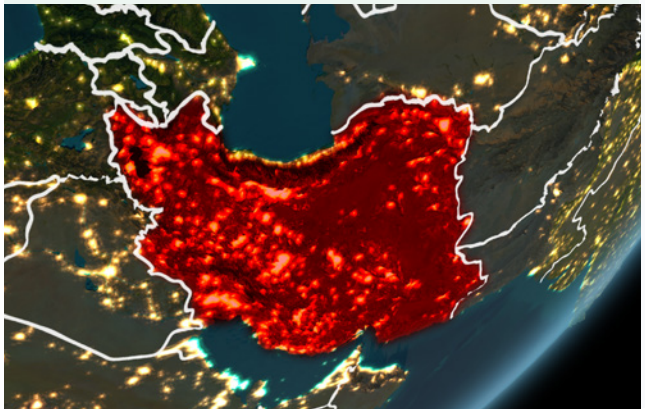
- **Prevalence of trade-based money laundering:** Iranian illicit networks' reliance on imports and exports to circumvent sanctions and carry out business has also created widespread opportunities for trade-based money laundering. Mis-invoicing, over- and under-shipment of goods and the use of multiple intermediaries allow actors to disguise the true value and origin of transactions. This practice is especially prevalent in sectors like petrochemicals, metals and consumer goods. Trade-based money laundering facilitates cross-border flow of illicit funds, evasion of customs duties and layering of proceeds, making it one of the most significant drivers of financial crime risk in the country.

- **Use of Foreign Intermediaries in High-Risk Jurisdictions:** Iranian illicit financial and trade networks often use counterparties that route transactions through intermediaries, trading houses or logistics firms in countries such as China or Russia, where opaque corporate structures and limited financial transparency can mask Iranian ownership or activity. Both illicit networks in China and Russia have developed increasingly sophisticated methods to operate outside Western financial channels, including alternative payment systems, layered corporate structures and state-tolerated grey-market networks, which Iranian networks have increasingly looked to utilise as well.

Financial Crime Risk Overview

01 Money Laundering: High Risk

Iran's money laundering risk landscape remains among the highest globally, driven by longstanding FATF blacklisting, structural weaknesses in the country's AML/CFT framework and pervasive illicit finance networks shaped by sanctions pressure, regional transnational criminal operations and broader geopolitical dynamics. Key vulnerabilities include extensive use of shadow-banking networks, front and shell companies abroad (notably in the Gulf and East Asia), informal currency-exchange channels and opaque ownership structures. Trends indicate increasing sophistication in laundering tactics, including complex trade-based schemes and multi-jurisdictional financial layering. Domestic reforms such as Iran's recent AML/CFT action plan have yet to materially reduce these systemic risks.



02 Bribery & Corruption: High Risk

Iran faces high bribery and corruption risk, driven by an entrenched system of patronage, cronyism and elite control, particularly by IRGC-linked entities. Its public sector is widely perceived as corrupt — in the 2024 Corruption Perceptions Index, Iran scored just 23 out of 100, placing it among the worst-ranked globally. Bribery and irregular payments are reportedly common in obtaining public contracts, licenses and government services, often to favour firms tied to powerful political or military elites. Iran does have a formal legal framework criminalising bribery, embezzlement and abuse of function but enforcement is weak and uneven. High-profile corruption scandals (e.g. embezzlement in the insurance sector and large-scale fraud in state procurement) illustrate systemic vulnerabilities, including the use of front companies by the IRGC to siphon off financial assets. In short, Iran's corruption environment is deeply rooted, driven by political-economic power structures and constitutes a major risk for governance, financial integrity and foreign investment.

03 Terrorist Financing: High Risk

Iran's terrorist and proliferation financing risks are extremely high - shaped by some Iranian actors' longstanding support for designated terrorist organisations, as well as the country's weak regulatory oversight and structural vulnerabilities in its financial system. The IRGC and affiliated entities are central conduits for funding groups such as Hezbollah, Hamas and regional militias, often using complex networks of front companies, charities and informal money-transfer systems to move funds across borders. Sanctions and international isolation have amplified reliance on opaque channels, including trade-based laundering and informal hawala systems, which obscure the origin and destination of funds. Additionally, limited beneficial ownership transparency, underdeveloped financial intelligence capabilities, and gaps in enforcement create systemic vulnerabilities that allow terrorist financing to persist largely undetected.

Iran's proliferation financing risks are also underpinned by its shadow-banking networks, deceptive trade-and-financial practices and the pivotal role of state and IRGC-linked entities in procuring components for its weapons programs. Its use of exchange houses and foreign front companies facilitates the laundering of oil revenues into foreign currency that is then directed toward procurement of advanced weapons systems. The FATF continues to designate Iran as a jurisdiction of high concern for proliferation financing, urging enhanced due diligence and countermeasures by financial institutions. Higher-risk typologies also include the procurement of missile components and dual-use technology, as well as the use of front companies to facilitate transactions disguised as legitimate commercial trade.

04 Sanctions Evasion: High Risk

Iran faces very high sanctions evasion risk, driven by long-standing sanctions against the country and its reliance on covert financial and commercial networks to circumvent these restrictions. To sustain revenue generation and international trade — particularly oil exports — and procure restricted goods, Iran employs a wide array of evasion techniques, including the use of front and shell companies, complex trade-based schemes, falsified shipping documentation and vessel-identity manipulation (such as flag-hopping, AIS spoofing, and ship-to-ship transfers).

IRGC-linked actors and state-affiliated intermediaries often play a central role in orchestrating these operations, leveraging foreign facilitators and offshore jurisdictions to obscure beneficial ownership and payment trails. Sanctions pressure also drives the use of informal financial channels, shadow-banking networks and third-country brokers to move funds outside the formal banking system. Weak regulatory oversight, extensive financial secrecy and entrenched corruption further enable these practices, while ongoing geopolitical tensions incentivise continual adaptation and increasing sophistication in Iran's evasion methods.

05 Fraud: Medium-High Risk

Cyber-fraud and consumer and business-targeted fraud are growing risk areas in Iran, driven by high internet and social media adoption, weak cybersecurity controls, and limited regulatory oversight of online financial activity. Cyber-enabled schemes such as phishing and social-engineering scams, account-takeover attacks and fake investment opportunities have become increasingly common, exploiting gaps in banking security, including digital services and lower public awareness. Businesses face heightened exposure to business-email-compromise (BEC) attacks that target payment systems and sensitive commercial data. The widespread use of unregulated online marketplaces, informal digital payment channels and encrypted messaging apps also facilitates fraudulent advertising, counterfeit goods sales and identity theft. Weak enforcement and slow incident response allow cyber-fraud networks to operate with relative impunity.

06 Tax Crime: Medium-High Risk

Iran faces medium-high tax crime risk, driven by structural weaknesses in tax administration, extensive use of the informal economy and pervasive corruption that undermines enforcement. A large share of economic activity — including cash-based businesses and informal trading networks — remains outside the formal tax net, creating substantial opportunities for tax evasion and fraudulent reporting. Weak auditing capacity, limited data-sharing across government agencies and insufficient digitalisation hinder the detection of under-reporting or trade-based tax fraud. Opaque tax exemptions for powerful institutions - including religious foundations and military-affiliated entities - create loopholes and incentives for concealment. In all, these vulnerabilities contribute to a high-risk environment where tax crime is systemic and difficult to combat.

07 Financial Secrecy: Medium-High Risk

Iran faces medium-high financial secrecy risk, underpinned by opaque ownership structures, limited public access to corporate and financial information and weak enforcement of transparency requirements across the banking, commercial and charitable sectors. Beneficial ownership disclosure is minimal, enabling front companies, quasi-state enterprises and IRGC-linked firms to mask control and move funds with limited scrutiny. Informal financial channels — including exchange houses, hawala networks and unregulated money-service businesses — further obscure the origin, purpose and destination of transactions. Sanctions-driven isolation reinforces these secrecy practices by pushing financial activity into offshore jurisdictions, shadow-banking networks and complex trade-based schemes designed to evade detection.

04 Drug and Weapons Trafficking: High Risk

Drug and weapons trafficking risks are very high in Iran due to the country's strategic geography and the presence of entrenched regional criminal networks. Positioned between major drug-producing areas, conflict zones and lucrative consumer markets, Iran — along with Afghanistan and Pakistan as the "Golden Crescent" region — serves as a key conduit for opium, methamphetamine other synthetic drugs such as Captagon, cannabis and precursor chemicals. Decades-old smuggling networks, compounded by the involvement of non-state armed groups, insurgents, and corrupt or state-linked officials, further heighten these risks. Although Iran invests heavily in counter-narcotics operations, corruption and rent-seeking among some security, border and customs personnel create vulnerabilities that facilitate illicit flows, while regional militant groups often use trafficking to fund their activities. Together, these dynamics fuel cross-border instability, sustain armed groups and expand transnational criminal markets across the region.

Weapons trafficking is similarly significant: Iran's production, stockpiling and covert transfer of arms to regional proxy groups contribute to both outbound illicit flows and the circulation of arms within the country. Weak border controls in remote regions, corruption among enforcement personnel and sophisticated smuggling methods — including concealed shipments, use of front companies and maritime routes — exacerbate these risks. Sanctions pressure and regional conflict dynamics further incentivise illicit trade as a revenue stream and political tool, making drug and weapons trafficking persistent, deeply embedded challenges within Iran's broader criminal-risk landscape.

05 Modern Slavery & Human Trafficking: High Risk

Iran faces significant modern slavery and human trafficking risks, driven in large part by economic hardship, regional instability and limited institutional capacity to detect and prevent exploitation. Forced labour risks are elevated among undocumented migrant workers and refugees, particularly Afghans, who often face debt bondage, coercive labour conditions and restrictions on movement due to their irregular status and limited legal recourse. Women and children are vulnerable to exploitation in domestic work, forced marriage and sexual trafficking, exacerbated by poverty, displacement and gaps in social-protection systems. Iran's role as both a source, transit and destination country for trafficking is reinforced by porous borders, corruption among some local officials and the presence of organised criminal networks operating across the region. These structural and socioeconomic pressures make modern slavery and human trafficking persistent and difficult-to-address risks in Iran's human rights landscape.

06 Cybercrime: High Risk

Iran faces an expanding cybercrime risk landscape, driven by growing digital adoption, a large informal digital economy and uneven cybersecurity maturity. Cyber-criminal activity ranges from financially motivated attacks, such as ransomware and data breaches, to broader malicious conduct, including hack-and-leak operations and disruption of critical services. Both domestic and foreign cyber-criminal groups operate in this ecosystem, exploiting outdated IT infrastructure (due in large part to sanctions-driven technological isolation) which limits access to advanced cybersecurity tools and enforcement capacity. Consumers and businesses are frequent targets due to widespread use of insecure apps, pirated software and unregulated online platforms. Iran also faces foreign cybercrime and cyber-espionage threats targeting its government and critical infrastructure, including foreign state-sponsored groups, hacktivists and cybercriminal networks carrying out attacks against government ministries, defence organisations, energy facilities and key industrial sectors.

07 Environmental Crime: Medium Risk

Environmental crime risks are growing in the country, driven by weak regulatory oversight, corruption and the exploitation of natural resources amid ongoing economic pressures. Most notably, the country faces high risks related to natural resource trafficking and oil smuggling, driven by sanctions pressure, entrenched black market networks and the strategic importance of hydrocarbons to the country's economy. Large volumes of crude oil and petrochemicals are diverted into illicit channels through ship-to-ship transfers, falsified cargo documentation, shell companies and vessel identity manipulation - methods often coordinated by IRGC-linked networks and foreign intermediaries.

Beyond oil, illegal logging, wildlife trafficking and unregulated hunting threaten biodiversity, while illicit sand and soil extraction contribute to land degradation and desertification. Water-related crimes, such as unauthorised well drilling, illegal diversion of rivers and black-market water trading, are also of note, due to chronic water scarcity and mismanagement. Limited enforcement capacity and inconsistent penalties enable these crimes to persist.

Key Financial Crime Watchpoints

Iran presents a complex and high-intensity financial crime environment shaped by sanctions pressure, entrenched illicit networks, opaque ownership structures, and systemic governance weaknesses. Companies considering business in Iran or with Iranian-linked entities or associates should first assess whether such activity is legally permissible under the sanctions regimes and regulatory frameworks of the jurisdictions in which they operate. Firms should also factor in Iran's continued blacklisting by the FATF, which calls on regulated entities to apply enhanced due diligence and other countermeasures when engaging with Iranian entities.

Those that are legally able to engage face heightened exposure across multiple risk areas, including sanctions evasion, proliferation financing, cyber-enabled fraud, corruption, and trafficking. The list below highlights key financial crime threats and red flags to support informed risk assessment and enhanced due diligence.

- **Opaque Ownership and State/IRGC Links:** Organisations should scrutinise counterparties for hidden beneficial owners, front companies or affiliations with IRGC-linked entities, state-owned enterprises or politically exposed networks that dominate key sectors such as energy and finance
- **Use of Informal or Non-Transparent Financial Channels:** Reliance on exchange houses, hawala networks, shadow-banking structures and cash-based transactions is common and often used to obscure sanctions evasion, money laundering or proliferation financing.
- **Unusual Trade or Shipping Patterns:** Red flags include complex or circuitous trade routes, inconsistent cargo documentation, ship-to-ship transfers, AIS manipulation and mismatches between goods, routes or pricing — all of which are highly relevant for oil, petrochemicals and dual-use goods smuggling and trafficking.
- **Use of Foreign Intermediaries in High-Risk Jurisdictions:** Organisations should be alert to counterparties operating through intermediaries, trading houses, logistics firms or shell companies based in jurisdictions with similar geopolitical dynamics or limited transparency. These networks are frequently used to disguise Iranian ownership, facilitate sanctions evasion, procure dual-use goods or reroute payments through opaque offshore channels.
- **Cybersecurity Weaknesses and Digital Fraud Exposure:** Organisations should watch for phishing attempts, compromised accounts, fraudulent digital platforms and cyber intrusions that exploit weak infrastructure and limited cyber controls.
- **High Corruption and Bribery Exposure in Procurement and Licensing:** Public-sector dealings often involve bribery risks, non-competitive tenders, irregular payments, expedited approvals or reliance on third-party "facilitators", all of which should trigger enhanced due diligence.
- **Risks of Involvement in Trafficking and Illicit Trade Networks:** Engagement in sectors like logistics, energy, mining, chemicals or border-adjacent commerce may expose companies to sanctions evasion, drug trafficking, natural resource smuggling or weapons-related supply chains - and associated financial crime risks.
- **Labour and Human-Rights Vulnerabilities in Supply Chains:** Engagement in sectors like logistics, energy, mining, chemicals or border-adjacent commerce may expose companies to sanctions evasion, drug trafficking, natural resource smuggling or weapons-related supply chains - and associated financial crime risks.

Next Steps: Navigating the 2026 Iran Risk Landscape

The early months of 2026 have underscored how rapidly Iran's financial crime risk landscape can evolve. Escalating geopolitical tensions, domestic uncertainty, and conflict-driven threats are creating immediate and far-reaching implications for businesses and individuals worldwide. At the same time, this shifting environment reflects the persistence of a highly resilient illicit financial ecosystem in Iran — one shaped over decades by sanctions, sustained economic pressure, and complex geopolitical and security dynamics.

This is why understanding the threat landscape is so important. Organisations need to act now, making sure their teams understand emerging risks, and that the necessary controls and processes are in place to keep up with a fast-changing environment.
That's where Themis comes in. We help organisations stay one step ahead with a mix of threat intelligence, training, regulatory scanning, and risk management. Our platform adds an extra layer of protection, giving teams the tools to identify and stop threats in real time before they escalate.

In today's complex risk environment, taking a proactive, intelligence-led approach to compliance and risk management is the only real option. By combining threat-based research, sanctions insights, and technology-enabled monitoring, organisations can spot risks earlier, make smarter decisions, and respond more effectively.

Next Steps: Key Actions for Navigating Iran-Related Risks

- **Conduct thorough due diligence** on all clients, suppliers, partners, and counterparties to identify and mitigate any potential links to Iranian threats.
- **Review and update sanctions and financial crime controls**, ensuring screening and monitoring processes are robust and aligned with current regulations.
- **Integrate intelligence-led insights** into operational and compliance workflows to anticipate emerging risks and act proactively.
- **Educate senior management and staff** on the organisation's specific risk environment, leveraging threat-based research, training, and scenario planning.
- **Engage trusted advisors** to update your organisation's risk profile and optimise technology tools, ensuring your risk management capabilities remain ahead of evolving threats.

Risk Area	Recommended Actions	How Themis Can Help
Sanctions & State-Linked Actors	Maintain up-to-date screening, rescreening, and due diligence; track evolving sanctions and designations.	Dynamic sanctions monitoring, PEP and high-risk counterparty screening, tailored compliance alerts.
Illicit Financial Networks	Conduct horizon scanning for Iranian-linked counterparties; assess exposure in high-risk sectors; monitor shadow networks and illicit finance flows.	FATF notes improved sectoral risk understanding, proportionate sanctions on FIs/DNFBPs, and increased STRs; national coordination and sector updates featured in EO AML/CTF's first Annual Report (Jun 2024)
Cybersecurity & Geopolitical Threats	Enhance incident response plans; monitor for retaliatory attacks; secure IT infrastructure against ransomware, data breaches, and hack-and-leak campaigns.	Intelligence on Iran-linked cyber activity, analysis of proxy threats, and monitoring of critical infrastructure risks.
Supply Chain & Regional Exposure	Map regional partners and vendors; identify trade-based threats and indirect exposure points; implement enhanced due diligence for supply chain.	Country and sector-specific risk assessments, supply chain mapping, and ongoing monitoring for high-risk connections.
Operational Resilience	Embed intelligence-driven risk insights into decision-making; adopt anticipatory controls; update protocols as the situation evolves.	Integrates research, sanctions insight, and monitoring technology into existing compliance and operational workflows for proactive risk management.

Our experts provide end-to-end support across financial crime, sanctions, cyber risk, compliance, and geopolitical threat monitoring.

Reach out to learn how we can help you adopt a more anticipatory, intelligence-driven approach to Iran-related risk, strengthen compliance, and safeguard operations in a rapidly evolving environment.

If you are concerned about any of the threats outlined in this country risk report, or if you would like tailored support in strengthening your organisation's resilience, please contact us. Themis offers Board level and Senior Management threat intelligence briefings, where our analysts meet with leadership teams to share the latest intelligence, outline evolving threat trajectories, and provide practical, sector-specific guidance for bolstering protective frameworks.

Get in Contact

click here

How Themis Can Help

Themis aims to be a leader in applying AI-led solutions to the problems of financial crime, and we are uniquely placed to do so. With strong working relationships with governments and businesses of many shapes and sizes, our software is developed with the needs of the whole financial crime compliance ecosystem in mind. By combining a focus on innovative technology with leading human intelligence and insight, Themis is capable of not only meeting those needs as they currently are but also anticipating them as they evolve in an uncertain future.

Our Reports and Services

Enjoyed this briefing? Keen for a more detailed analysis that's specific to your business? We deliver longer, bespoke reports and executive briefings about specific countries or sectors. Whether you're investing in new markets, expanding your own footprint or ensuring your financial crime country risk assessments align with the Wolfsberg Group's principles, our Risk Intelligence team can help. We specialise in complex, strategic projects where financial crime risks are new, emerging, or poorly understood.

Get in touch to find out more.

Our Team of Experts

Nadia O'Shaughnessy
Head of Insight
nos@wearethemis.com

Olivia Dakeyne
Principal, Research
od@wearethemis.com

Eliza Thompson
Financial Crime Researcher
et@wearethemis.com

Henry Wyard
Senior Policy Analyst
hjw@wearethemis.com

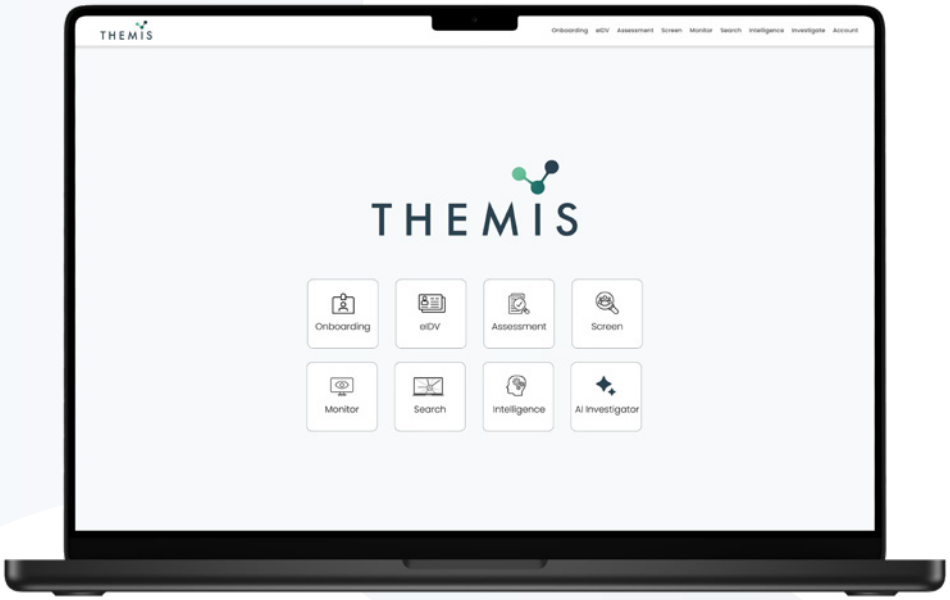
Nikhil Gandesha
Global Financial Crime Training Lead
ng@wearethemis.com

Emily Hsu
Financial and Environmental Crime Researcher
eh@wearethemis.com

Discover Other Country Risk Briefings

Research-driven analysis that informs and inspires action to tackle financial crime

Discover all



THEMIS

UK: +44 (0) 20 8064 1724 | UAE: +971 (0) 58 526 8765

info@wearethemis.com

www.wearethemis.com

Certified B Corporation