SPACE FINANCIAL SERVICES AUTHORITY

SFSA

INTERIM GUIDANCE NOTE

IGN-003

AML/CFT Framework for Space Economy Financial Institutions — Detailed Guidance

Document reference	SFSA/IGN-003/2025
Status	In Force — Interim Standard
Issued by	Gilles Rollet, Secretary General
Date of issue	[Date]
Effective date	Date of issue
Supersedes	N/A — supplements IGN-001 Section 6
Next review	12 months from date of issue
Applies to	All SFSA-Authorised Institutions and Applicants
Read alongside	SFSA IGN-001 — Baseline Standards

Executive Summary

This Interim Guidance Note (IGN-003) provides detailed AML/CFT guidance for SFSA-Authorised Institutions, expanding on the baseline requirements set out in IGN-001 Section 6. It addresses the specific money laundering and terrorist financing risks inherent in the space economy — risks that are poorly understood by conventional AML frameworks and that SFSA-Authorised Institutions must address specifically and explicitly.

IGN-003 covers: the SFSA risk-based approach to AML/CFT; a detailed space economy risk matrix; enhanced due diligence requirements for high-risk space economy client categories; transaction monitoring adapted for space economy financial flows; correspondent banking and cross-border considerations; and the SFSA's expectations for MLRO qualifications and the annual AML/CFT audit.

NOTE IGN-003 does not substitute for applicable national AML/CFT law. SFSA-Authorised Institutions must comply with all applicable FATF Recommendations, national AML legislation, and SRO/supervisory body requirements. Where SFSA standards are more stringent, the SFSA standard applies as between the institution and the SFSA.

PLAIN TERMS IGN-003 sits on top of your national AML/CFT law — it does not replace it. Meet every applicable FATF Recommendation, national AML law, and supervisory requirement that applies to you. Where SFSA asks for more, meet the SFSA standard too, as between you and us.

Section 1 — The SFSA Risk-Based Approach

1.1 Principle

The SFSA adopts a risk-based approach to AML/CFT, consistent with FATF Recommendation 1. This means that SFSA-Authorised Institutions must identify, assess, and understand the money laundering and terrorist financing risks to which they are exposed, and take AML/CFT measures commensurate with those risks. A one-size-fits-all approach is not acceptable.

PLAIN TERMS In practice: know your specific money-laundering and terrorist-financing risks, and size your controls to match them. One-size-fits-all does not work here.

1.2 The Space Economy AML/CFT Challenge

The space economy presents AML/CFT risk characteristics that do not appear in standard banking risk frameworks. These are not marginal variations on familiar risks — they are structurally novel. SFSA-Authorised Institutions must treat these as primary risk categories, not edge cases.

The five primary novel risk categories in the space economy are:

Risk Category	Nature of Risk	Why Novel
Dual-use technology	Space technology — launch vehicles, propulsion, guidance, satellite components — has direct military applications and is subject to export controls (ITAR, EAR, EU dual-use). Financial flows related to dual-use technology may be subject to sanctions or export control violations that are not apparent from standard KYC.	Standard banking AML frameworks do not include export control screening as a core AML function. In the space economy it is essential.
Pre-revenue clients	Most space economy companies are pre-revenue at client onboarding — their funding comes from investors, grants, and government contracts, not commercial revenues. Standard source-of-funds verification is inapplicable.	Creates structural difficulty in verifying legitimate source of funds using conventional methods.
Sovereign and governmental counterparties	Many space transactions involve national space agencies, sovereign launch operators, and state-linked satellite companies. These are PEPs or PEP-adjacent entities by definition.	Standard PEP frameworks cover political figures, not institutional sovereigns active in commercial space.
Multi-jurisdictional	A single space economy	Standard correspondent banking

Risk Category	Nature of Risk	Why Novel
complexity	transaction may involve counterparties in multiple jurisdictions, assets in orbit (no terrestrial jurisdiction), insurance in Bermuda or London, and settlement in USD.	AML frameworks are not designed for transactions whose underlying asset exists in international space.
In-space asset valuation	As in-space manufacturing, resource extraction, and orbital infrastructure develop, financial transactions will involve assets whose valuation is opaque, unregulated, and not covered by any terrestrial valuation standard.	Creates risk of asset-based money laundering using in-space assets as the vehicle — analogous to real estate money laundering but with no established valuation or registration framework.

Section 2 — Space Economy Risk Matrix

2.1 Mandatory Risk Assessment

Every SFSA-Authorised Institution must maintain a written Space Economy AML/CFT Risk Assessment, updated at least annually, that maps the institution's specific client base, product set, and geographic exposure against the risk categories in this section. The risk assessment must be approved by the Board and reviewed by the MLRO.

2.2 Client Risk Matrix

Client Category	Inherent Risk Level	Required Due Diligence
Commercial satellite operator — established revenue	Low–Medium	Standard CDD — UBO verification, source of funds, business description
Launch vehicle operator — pre-revenue startup	High	Enhanced CDD — investor verification, cap table review, export control check, government contract review
National space agency — Western/OECD	Medium	Enhanced CDD — sovereign PEP analysis, mandate verification, government approval confirmation
National space agency — non-OECD or sanctioned jurisdiction	Very High or Prohibited	EDD + SFSA Secretariat notification — or decline
Space tourism operator	Medium	Enhanced CDD — passenger screening protocols, source of wealth for UHNW participants
In-space resource extraction company	High	Enhanced CDD — regulatory status, government licences, environmental approvals
Space technology supplier (dual-use components)	Very High	EDD + export control screening — ITAR/EAR check, end-user certificate, government clearance
Space-focused VC or family office	Medium	Standard CDD + investor source of wealth
Orbital platform / space station operator	High	Enhanced CDD — multi-jurisdiction analysis, government relationships, technology classification
Individual space economy founder / executive	Low–Medium	Standard CDD — PEP check if government-linked, source of wealth if UHNW

2.3 Product and Channel Risk

Product / Channel	Risk Factors	Mitigant
Wire transfers — space economy payments	Cross-border, multi-currency, complex counterparties	Correspondent bank screening, purpose verification

Product / Channel	Risk Factors	Mitigant
Trade finance — launch contracts	Large value, dual-use equipment, foreign counterparties	End-user certificate, export control check, letter of credit documentation
FX — orbital transaction settlement	Novel instrument, no established price reference	Transaction monitoring, rate benchmarking
Deposits — pre-revenue space companies	Funds sourced from investors, not revenues	Investor verification, cap table review, grant documentation
Private banking — space economy UHNW	High wealth, complex structures, international	Source of wealth, SOF, enhanced ongoing monitoring
Digital assets — future orbital settlement	Novel, pseudonymous, cross-jurisdictional	Enhanced screening, wallet analysis, DeFi exposure assessment

Section 3 — Customer Due Diligence — Detailed Standards

3.1 CDD Trigger Events

SFSA-Authorised Institutions must conduct CDD at the following trigger points:

- At onboarding — before establishing any client relationship or processing any transaction
- At each periodic review — annually for standard risk, every 6 months for high risk, every 3 months for very high risk
- Upon any material change in client profile — change of UBO, change of business activity, change of jurisdiction, significant change in transaction patterns
- Upon any suspicious activity indicator — regardless of scheduled review date
- Upon a SAR filing — full CDD refresh required before any further transactions

3.2 Standard CDD — Corporate Clients

For all corporate space economy clients, the following minimum documentation must be obtained and verified:

- Certificate of incorporation or equivalent — certified copy
- Articles of association / constitutional documents
- Current commercial register extract or equivalent
- UBO declaration — all persons with direct or indirect ownership or control at or above 10%
- Certified passport copies for all UBOs, directors, and authorised signatories
- Proof of address for all UBOs and directors — utility bill, lease, or equivalent, dated within 3 months
- Description of space economy activities — what the company does, what assets it holds, who its customers are
- Source of funds declaration — how does money come into the account? (investor capital, government grants, commercial revenues, or a combination)
- Government licences and regulatory approvals relevant to space activities — launch licence, spectrum licence, orbital slot rights, export licences

3.3 Enhanced Due Diligence — Triggers and Requirements

Enhanced Due Diligence (EDD) is mandatory — not discretionary — for all clients that meet any of the following criteria:

- Any client classified as High or Very High risk in the risk matrix (Section 2.2)
- Any PEP or entity majority-owned or controlled by a PEP or government
- Any client domiciled in, or with material operations in, a FATF high-risk or monitored jurisdiction
- Any client whose activities involve dual-use technology (ITAR/EAR-controlled items)
- Any client where the source of funds cannot be verified by standard means
- Any client where the initial risk assessment raised unresolved questions

EDD must include, in addition to standard CDD:

- Senior management approval — EDD relationships must be approved by a member of senior management (not just the MLRO)
- Enhanced source of wealth analysis — for UHNW individuals, a full wealth biography is required
- Enhanced source of funds — bank statements or investor statements for the last 12 months minimum
- Reference checks — at least two independent references from recognised financial institutions or professional advisers
- Export control screening — check against ITAR/EAR Entity Lists, Denied Parties Lists, and relevant national export control registers
- Media and adverse information search — structured open-source search using a recognised screening tool
- More frequent ongoing monitoring — as specified in Section 2.2

3.4 Dual-Use Technology — Special Protocol

Where a client's activities involve dual-use technology — including satellite components, launch vehicle systems, propulsion technology, guidance and navigation systems, and remote sensing equipment — SFSA-Authorised Institutions must implement the following special protocol:

1. Identify whether the client's technology is controlled under ITAR (US International Traffic in Arms Regulations), EAR (US Export Administration Regulations), EU Dual-Use Regulation 2021/821, or applicable national export control regimes
2. Obtain copies of all relevant export licences and end-user certificates for any transactions involving controlled technology
3. Screen all counterparties in dual-use transactions against: US Denied Parties Lists (BIS Entity List, OFAC SDN List, State Department ITAR Debarred List); EU Consolidated Sanctions List; Swiss SECO sanctions list; UN Security Council Consolidated List
4. Where controlled technology is involved, obtain a written legal opinion from a qualified export control lawyer confirming that the proposed transaction does not violate applicable export control regimes
5. Escalate all dual-use technology clients to MLRO for approval before onboarding, regardless of other risk indicators

REQUIREMENT No SFSA-Authorised Institution may provide financial services to a client whose dual-use technology activities are subject to an active export control violation investigation, a denial order, or a sanctions designation. If such a designation is identified post-onboarding, the institution must immediately freeze the account, file a SAR, and notify the SFSA Secretariat.

Section 4 — Transaction Monitoring

4.1 Mandatory Transaction Monitoring Programme

Every SFSA-Authorised Institution must implement a transaction monitoring programme appropriate to the volume, complexity, and risk profile of its business. The programme must be documented, reviewed annually, and approved by the Board.

4.2 Space Economy Transaction Monitoring Red Flags

In addition to standard AML transaction monitoring red flags, SFSA-Authorised Institutions must monitor specifically for the following space economy indicators:

Red Flag	Indicator	Required Response
Launch payment spike	Large payment to a launch service provider within 30 days of a previously unannounced launch	Verify launch contract; confirm export licences; escalate to MLRO if unverified
Unexplained technology payment	Payment to a technology supplier not previously identified in CDD as a counterparty	Request invoice and end-user certificate; export control check; escalate if dual-use
Government agency roundtrip	Payment to government agency followed by return payment of similar amount	Verify legitimate contractual basis; escalate if no clear contract
Pre-revenue funding spike	Large deposit from a previously unknown investor into a pre-revenue company	Verify investor identity and source of funds; update CDD
Sanctions jurisdiction routing	Payment routed through a correspondent bank in a high-risk or sanctioned jurisdiction	Block and investigate; file SAR if no legitimate explanation
Orbital asset transfer	Transaction described as payment for orbital slot, satellite constellation rights, or in-space infrastructure	Verify regulatory basis for transaction; obtain valuation; escalate — no established market price reference
Rapid round-tripping	Funds received and immediately transferred out to a third party without apparent commercial purpose	Freeze and investigate; file SAR if no explanation within 24 hours
Digital asset conversion	Conversion of space economy proceeds to digital assets without disclosed purpose	Enhanced monitoring; verify exchange, wallet, and purpose

4.3 Monitoring Thresholds

SFSA-Authorised Institutions must apply enhanced scrutiny to all transactions above the following thresholds:

- Single transaction: CHF / € / USD 50,000 or equivalent — require transaction purpose documentation
- Cumulative transactions with a single counterparty in 30 days: CHF 250,000 — trigger relationship review
- Cash or crypto equivalent transactions: CHF 10,000 — automatic MLRO notification
- International wire transfers to non-OECD jurisdictions: CHF 25,000 — enhanced beneficiary screening

4.4 Suspicious Activity Reporting

Where a transaction monitoring alert is raised and cannot be satisfactorily explained within the timeframes set out in Section 4.2, the MLRO must assess whether a SAR is required under applicable national law. The SFSA additionally requires:

- All SARs filed with national financial intelligence units must be reported to the SFSA Secretariat within 5 business days of filing — by reference number only, not by content, to preserve tipping-off protections
- A log of all SAR assessments — including those where a decision was made not to file — must be maintained by the MLRO and made available to the SFSA on request
- The MLRO must report to the Board on SAR activity — in aggregate and anonymised form — at least quarterly

PLAIN TERMS Filed a SAR with your national financial intelligence unit? Tell the SFSA Secretariat within 5 business days — the reference number only, never the content. That protects the tipping-off rules that make the SAR system work.

Section 5 — Sanctions Screening

5.1 Mandatory Sanctions Lists

Every SFSA-Authorised Institution must screen all clients, counterparties, beneficial owners, and transactions against the following sanctions lists as a minimum:

- UN Security Council Consolidated Sanctions List
- EU Consolidated Sanctions List (including asset freezes and travel bans)
- Swiss SECO Sanctions List
- US OFAC Specially Designated Nationals (SDN) List
- US BIS Entity List and Denied Parties Lists
- UK Office of Financial Sanctions Implementation (OFSI) Consolidated List
- Any additional lists required by national law in the jurisdiction of operation

5.2 Screening Frequency

- All new clients and counterparties: screened before onboarding — no exceptions
- All existing clients: re-screened in real time or within 24 hours of any list update
- All transactions: screened at point of processing — payments must not be released without clean screening result
- Periodic full-portfolio rescreening: not less than monthly

5.3 Space Economy Sanctions Considerations

The space economy has specific sanctions exposure that standard banking operations do not face:

- National space programmes of sanctioned states — Russia (Roscosmos), Iran, North Korea, and their commercial entities — are subject to comprehensive sanctions. Any financial relationship with these entities, their subsidiaries, or their joint venture partners is prohibited.
- Dual-use technology export to sanctioned states is an aggravated sanctions violation — the combination of sanctions breach and export control violation creates extreme legal and reputational risk.
- Orbital assets — satellite transponders, orbital slot assignments — may be owned by sanctioned entities even where the operating company appears clean. Verify ultimate ownership of all orbital assets involved in a transaction.

RISK ALERT Any institution that processes a transaction involving a sanctioned space entity — even inadvertently — faces the risk of criminal prosecution, regulatory action, and immediate loss of SFSA Authorisation. Zero tolerance applies. When in doubt, decline and escalate.

Section 6 — MLRO Qualifications and Governance

6.1 MLRO Appointment

Every SFSA-Authorised Institution must designate a qualified Money Laundering Reporting Officer (MLRO). The MLRO must:

- Be a member of senior management or report directly to senior management — the MLRO must have sufficient seniority and independence to discharge their function effectively
- Hold an appropriate AML/CFT qualification — ICA Diploma in AML, CAMS (Certified Anti-Money Laundering Specialist), or equivalent recognised qualification
- Have a minimum of 5 years of AML/CFT compliance experience in financial services
- Have read and understood IGN-001 and IGN-003 in full and confirmed this to the Board in writing
- Be approved by the SFSA Secretariat as fit-and-proper for the MLRO function prior to appointment

PLAIN TERMS Your MLRO needs enough seniority and independence to actually do the job — not just hold the title.

6.2 MLRO Responsibilities

- Maintains and updates the institution's AML/CFT policy and procedures
- Reviews and approves all EDD client onboardings
- Makes all SAR filing decisions — the MLRO is the sole person authorised to file or decide not to file a SAR
- Manages the transaction monitoring programme — reviews alerts, approves escalation, documents decisions
- Delivers annual AML/CFT training to all relevant staff
- Reports to the Board quarterly on AML/CFT matters
- Manages the annual AML/CFT audit — appoints and liaises with the external AML auditor
- Maintains the SAR log and all AML/CFT compliance records
- Acts as primary contact for the SFSA Secretariat on AML/CFT matters

6.3 Annual AML/CFT Audit

Every SFSA-Authorised Institution must commission an annual AML/CFT audit by an independent external auditor with appropriate AML/CFT expertise. The audit must cover:

- Assessment of the AML/CFT policy and procedures against applicable legal requirements and SFSA IGN-003 standards
- Testing of CDD files — sample review of client onboarding files for completeness and quality
- Transaction monitoring — assessment of the programme design and a sample review of alerts and decisions

- Sanctions screening — assessment of list coverage, screening frequency, and alert management
- MLRO governance — assessment of MLRO independence, reporting lines, and board engagement
- Training — confirmation that annual training was delivered and records maintained

The audit report must be submitted to the SFSA Secretariat within 30 days of completion, together with the institution's management response and remediation plan for any findings.

SPACE FINANCIAL SERVICES AUTHORITY

The world's first financial regulatory body dedicated to the space economy

Canton of Valais, Switzerland · sfsa.org · secretariat@sfsa.org