Q-KYC SXM - Executive Summary + Cost of Compliance

For the supervisory meeting with FIU/MOT and CBCS

Q-KYC SXM - 4MFESW / DNFBP Tenant

2026-06-16

Table of Contents

Q-KYC SXM — Executive Summary 1

1. What Q-KYC SXM is, in one paragraph 1

2. What it does NOT do, in one paragraph 2

3. Why this matters to the FIU and CBCS 2

4. Defensive design choices the regulator will care about 2

5. Numbers, today 4

Pricing 4

Q-KYC SXM fees 4

What the tier differences actually are 5

Your other compliance costs (independent of Q-KYC) 6

How the alternatives price 6

Disclosures 6

Q-KYC SXM — Executive Summary

For: FIU/MOT and CBCS, in advance of the supervisory meeting with the Tenant Firm (configured at install) **From:** the Tenant Firm (configured at install), Sint Maarten **Date:** 2026-05-31 **System version:** Q-KYC SXM v0.6.11

---

1. What Q-KYC SXM is, in one paragraph

Q-KYC SXM is an on-premise AML/CFT operating system for a single DNFBP. It collects client identity and ownership data, screens it against OFAC / UN / EU sanctions lists in real time, scores risk against FATF Recommendations 10 and 12, generates regulator-ready artifacts (goAML 4.0 SAR/CTR, KvK UBO filing, CBCS Annual Report), and writes every action to a hash-chained audit log that cannot be back-dated without detection. It runs on

a single Windows box in the firm's office. The MLRO is the only human with authority to file an SAR; the system enforces this with role-based access control.

2. What it does NOT do, in one paragraph

Q-KYC SXM does not auto-submit to any regulator today, because none of FIU/MOT, KvK SXM, or CBCS currently publish a programmatic intake to which it could submit. The MLRO downloads each artifact and files manually via the regulator's web portal or email; the receipt is then re-attached to the audit chain. Q-KYC SXM is also not a face- matching or liveness-detection service — those are scoped for a phase-2 Onfido/Sumsub integration. It does not transmit any client data off the firm's premises except when the MLRO chooses to file with a regulator.

3. Why this matters to the FIU and CBCS

For the **FIU**: every SAR the firm files via goAML is preceded by a case file that includes (a) the screening run that triggered it, with provider name, version, and snapshot hash; (b) the MLRO review decision with timestamp and a hash-chained audit trail; (c) the SAR XML draft itself. If the FIU later asks "how did you know this was suspicious?", the answer is reproducible from the artifact bundle. Tip-off lockdown is engaged automatically the moment a SAR is drafted (Wwft art. 23).

For **CBCS**: the system generates a one-shot Annual AML/CFT Compliance Report that aggregates entity count, risk distribution, case throughput, SAR count, sanctions-hit count, and the audit-chain integrity check — directly addressing CBCS Provisions & Guidelines section 6 reporting expectations. The report is reproducible to any historical date because every data point is sourced from immutable audit events.

For **the GDPR/AVG-aware regulator**: Q-KYC SXM operates an Article 30 processing register (`regulator_api_access_log`) that records every read of client data by an external regulator's pull token, with the specific data subject, timestamp, and bearer. The firm can produce a data-subject access response in under five minutes for any client.

4. Defensive design choices the regulator will care about

Concern	How Q-KYC SXM addresses it
Tampering with historical records	Hash-chained `audit_events` table; every row's `event_hash` includes the previous row's hash. Any post-hoc edit breaks the chain at the subsequent verifier call.
Tampering with stored documents	Documents are Fernet-encrypted at rest (key derived from the JWT secret via HKDF-SHA256). Plaintext SHA-256 stored separately; on download, the API decrypts, hashes, and refuses to serve if the hash

Concern	How Q-KYC SXM addresses it
	drifts.
Malware uploaded as a client document	Every upload is streamed through ClamAV (3.6M signatures, refreshed daily) before being written to disk. Infected files are refused with HTTP 422 and never persisted.
Fake or expired ID documents	ICAO 9303 MRZ parser validates every check digit on passports and national IDs at intake. Expired or check-digit-failing documents are flagged inline.
MLRO authority bypass	Drafting an SAR is gated by role-based access control. Only users with role `mlro` (or above) can call `/cases/{id}/sar-draft.xml`. Every successful and refused attempt is audit-chained.
Tip-off offence (Wwft art. 23)	The moment a SAR draft is created, the entity is set to `tipoff_locked=true`. The SPA hides outbound-communication actions while this flag is set. Releasing the lock requires role `mlro` or `super_admin` and is itself audit-logged.
Multi-jurisdictional clients (FATF R.10)	Selecting a second nationality on the Identity tab automatically bumps risk to medium and annotates the file for EDD review.
Periodic-review compliance (FATF R.10)	A daily scheduled task queues every entity whose `next_review_date` has passed; the MLRO sees a “Reviews Due” inbox.
Right to be forgotten / data retention	Retention period is set per regime (NOIS art. 33 = 10 years for SXM); a separate script can purge expired data and chains a deletion event.
Auditor independence	Role `independent_auditor` is read-only across every API endpoint via a global FastAPI dependency (`enforce_auditor_readonly`); cannot create cases, edit records, or submit reports.

5. Numbers, today

- **Sanctioned entries loaded**: 1,578,104 across OFAC SDN + UN Consolidated + EU Consolidated lists, refreshed nightly.
- **Audit chain depth**: integrity-checked from genesis to the most recent event on every regulator-facing read.
- **Encryption at rest**: 100% of documents (Fernet, ~256-bit symmetric key derived per-installation).
- **Lockout policy**: 5 failed logins → 15-minute lock per user.
- **MFA**: mandatory for roles `mlro`, `tenant_admin`, `super_admin` (TOTP, encrypted secret at rest).
- **Backup**: nightly pg_dump + document store + service env → encrypted zip; tested restore RTO < 5 minutes on a fresh host.
- **Languages**: operator UI + manual in EN / NL / FR / ES.

Pricing

Q-KYC SXM fees

Q-KYC's own fees — a one-time install plus a subscription. These are **separate** from the firm's other compliance costs (hardware, UPS, external audit, MLRO training), which exist regardless of which AML system you run (see "Your other compliance costs" below).

Prices in **EUR** (contractual). USD shown for cross-reference at EUR 1 = USD 1.1540 (ECB ref, 11 Jun 2026), rounded up to the next USD 100.

Tier	Active clients	Users incl.	One-time install	Monthly	Annual
Tier-1 — Sole practitioner	≤10	1	€1,500 (USD 1,800)	€60 (USD 100)	€720 (USD 900)
Tier-2 — Small firm	≤50	2	€2,500 (USD 2,900)	€200 (USD 300)	€2,400 (USD 2,800)
Tier-3 — Mid DNFBP / TCSP	≤500	10	€3,000 (USD 3,500)	€1,500 (USD 1,800)	€18,000 (USD 20,800)
Tier-4+	>500	—	project-based	project-based	project-based

The install fee excludes hardware and external subscriptions (e.g. cloud storage).

Founding-pilot offer: open to the first 10 subscribers. Minimum commitment 6 months; the full **25% off the annual subscription** (install not discounted) requires a 3-year commitment: Tier-1 €540/yr · Tier-2 €1,800/yr · Tier-3 €13,500/yr.

Additional users beyond the included count: +€720 (Tier-1) / +€1,200 (Tier-2) / +€1,800 (Tier-3) per user per year.

The full ladder is in the rate sheet (provided on request). All tiers ship identical regulatory substance — see "What the tier differences actually are" below; you do not get less compliance on a smaller tier.

What the tier differences actually are

What changes between Tier-1 / 2 / 3:

Line item	Tier-1	Tier-2	Tier-3
Hardware	Refurb mini-PC (Intel NUC i5 / equiv.)	Mini-PC i5, 16 GB RAM, 512 GB	Mini-PC i7, 32 GB RAM, 1 TB
UPS	600 VA	1000 VA	1500 VA
External backup	1 TB USB	2 TB USB	4 TB USB
Initial MLRO training	2 hrs remote	4 hrs hybrid	8 hrs on-site
Migration	Included (≤20 records via CSV)	Included (≤100 records)	Quoted separately above 100
Cloud backup quota	10 GB	25 GB	50 GB
Annual audit scope	Self-attestation + Q-KYC integrity check	Full external audit, ~1 day	Full external audit, 2-3 days
MS365 SMTP relay	0 (use personal mailbox + app password)	1 service mailbox	1 service mailbox + ticketing

What is **identical across all three tiers** (no compromise on the regulatory substance):

- ClamAV scanning of every uploaded file
- Fernet encryption at rest
- ICAO 9303 MRZ validation
- Hash-chained audit log
- OFAC + UN + EU sanctions data, refreshed daily
- Tip-off lockdown on SAR draft
- Role-based access control with MFA on privileged roles
- AVG/GDPR Art. 30 register on every regulator pull
- 4-language operator manual (EN/NL/FR/ES)

You do **not** get less compliance by choosing the smaller tier; you get the same software on less hardware with less audit days.

Your other compliance costs (independent of Q-KYC)

Beyond Q-KYC's fees above, a firm carries the usual cost of running an AML programme — a server, a UPS, off-site backup, external audit days, and MLRO continuing education. Those are the firm's own operational costs and depend on choices the firm makes (hardware spec, auditor, training provider); they are the same whichever AML system you run, so they are out of scope for this summary. See the per-tier hardware + operations spec (`HARDWARE-REQUIREMENTS`) for indicative figures.

How the alternatives price

The cloud-SaaS alternatives do not publish enterprise pricing. **ComplyAdvantage** publishes only a Starter tier (from USD 99/mo, ≤2,000 monitored entities); its enterprise tier is quote-only. **Napier** and **Quantexa** publish no pricing at all — both are enterprise contact-sales. All three are cloud-only and ship client data off-island. Q-KYC publishes its full price (above), runs on-premise, and keeps every byte inside SXM jurisdiction.

Disclosures

- **Currency:** Q-KYC fees are set in EUR (contractual); USD shown for cross-reference at EUR 1 = USD 1.1540 (ECB ref, 11 Jun 2026), rounded up to the next USD 100.
- **Pricing:** the founding-pilot discount (first 10 subscribers, 6-month minimum, full 25% off annual on a 3-year commitment) is the only discount; the install fee is not discounted. Tier-4+ (>500 clients) is project-based.
- **PEP-data note:** the free OFAC/UN/EU stack already covers sanctions screening; commercial PEP feeds are a *quality* upgrade, not a *compliance* requirement under CBCS P&G.

This summary is reproducible from the source markdown via the same pandoc + Word toolchain that generated the explainer manual.