Q-KYC SXM — Per-tier hardware, software & compliance-continuity requirements

Concrete minimum + recommended specs the customer needs to procure BEFORE Q-KYC SXM is installed. Includes the external costs and compliance-driven obligations that exist independently of the Q-KYC licence (UPS, off-site backup, etc).

Last revised: **2026-06-07**. Pricing in EUR ex-VAT, rounded.

Why these requirements exist

Driver	Source	What it demands
NOIS art. 33	Landsverordening Melding Ongebruikelijke Transacties	5-year retention of CDD records, *intact* (not corrupted, not partial)
LBP art. 14	Landsverordening Bescherming Persoonsgegevens	"Appropriate technical and organisational security measures" — proportional to the data sensitivity
CBCS P&G §6, §9	Provisions & Guidelines on AML/CFT	Business continuity, operational-risk management, demonstrable controls
Q-KYC hash chain	Internal architecture	Hash chain integrity requires graceful shutdown — interrupting a write mid-transaction could break the chain. The chain stays intact thanks to PostgreSQL WAL atomicity, but the supporting hardware needs UPS + safe-shutdown automation to make that guarantee real every time.

A CBCS supervisor will not ask "did you buy a UPS?". They will ask: **"Show me your business-continuity plan."** This document is the plan, broken down by firm size.

Tier S — Sole practitioner / 1-5 staff / <10 active clients

Profile: single MLRO, often the partner running the firm. Client volume is low; the system runs on one workstation in the office, accessible only from inside the firm.

Hardware — minimum

Component	Spec	Approx. EUR	Why
Computer	Windows 11 Pro desktop or mini-PC. Intel i5-12xxx / AMD Ryzen 5 5xxx or newer	600	OS-licence cost varies; Pro required for BitLocker + nssm services
RAM	16 GB DDR4 / DDR5	60	8 GB works but is uncomfortable; 16 GB is the practical floor
Storage (primary)	512 GB NVMe SSD	50	SSD is non-negotiable — PostgreSQL hash-chain inserts are write-heavy
Storage (backup)	1 TB external USB SSD (e.g. Samsung T7)	80	For the nightly local backup
UPS	APC Back-UPS BX700U-GR (700 VA / 390 W, 8 min runtime under typical load)	70	**Compliance-driven.** Without a UPS the audit chain depends on luck. Power cut during a write = potential WAL corruption.
Network	Gigabit-Ethernet to the office router; office router with reasonable consumer firewall	included	
Display	One monitor, FHD or better	120	
Subtotal hardware (one-off)		**~980**	

Hardware — recommended adds

Component	Spec	EUR
Mini-UPS for the router itself	APC Back-UPS Mini (~30 min)	50
Lockable IT cabinet or under-desk box	physical access control	60
Total recommended (one-off)		**~1,090**

Software — included with Q-KYC install

- Q-KYC SXM application + bundled PostgreSQL 18 + bundled Python
- ClamAV (~3.6 M signatures, daily refresh)
- Tesseract OCR + ICAO 9303 MRZ parser
- nssm (service manager)
- Caddy (HTTPS reverse proxy)
- Standalone `verify_audit_chain.ps1`

Software — customer provides

Item	EUR	Notes
Windows 11 Pro licence	0 (already on the PC)	If new PC, +180
Microsoft 365 / Outlook for the MLRO mailbox	already at the firm	
Antivirus on the OS (Windows Defender is sufficient)	0	Defender + ClamAV is double-layer

Backup architecture — 3-2-1 minimum

Copy	Where	Frequency	Retention	EUR/yr
1 — primary live	NVMe SSD in the workstation	continuous	5 yr (NOIS art. 33)	0
2 — local backup	external USB SSD (Samsung T7)	nightly automated	12 months rolling	one-off 80
3 — off-site	Backblaze B2 or pCloud encrypted	weekly automated	5 yr (NOIS art. 33)	**~60-120**

Total off-site backup cost: **~€60-120/yr** depending on retention policy + transfer volume.

Power-continuity profile

- **UPS runtime target:** ≥ 5 minutes under load. Enough time for the UPS daemon (APC PowerChute Personal Edition — free) to send a graceful-shutdown signal to

Windows. Windows shutdown triggers the Q-KYC-API nssm service to stop cleanly, which closes PostgreSQL connections and flushes the WAL.

- **Generator:** not required at Tier S.
- **Total time from power loss to clean shutdown:** ≤ 90 seconds.

Disaster recovery

Metric	Target	Implementation
RTO (Recovery Time Objective)	< 4 hours	Replacement PC + USB-SSD restore + verify audit chain
RPO (Recovery Point Objective)	< 24 hours	Nightly off-site backup
Backup verification	weekly	Automated `verify_audit_chain.ps1` against the off-site backup
Calamity scenarios covered	Fire, theft, hardware failure	NOT covered: long-power-outage > 4 hours (would need generator)

Total external CAPEX/OPEX for Tier S

Year 1	EUR
Hardware one-off	1,090
Backup software/cloud (12 months)	100
Power discipline (UPS replacement battery in year 3)	0
Year-1 external total	**~1,190**
Yr 2-5 annual external	**~100/yr**

Tier M — Small firm / 5-15 staff / 10-50 active clients

Profile: small accountancy, notarial practice, or boutique advocate firm with one MLRO and 2-5 compliance officers. Q-KYC is deployed on a dedicated office workstation that serves the firm's internal browsers. Possibly remote-access via the firm's VPN.

Hardware — minimum

Component	Spec	Approx. EUR	Why
Workstation	Windows 11 Pro mini-tower. i7-12700 / Ryzen 7 5800X	900	Dedicated machine, not the partner's daily-driver
RAM	32 GB	100	Multi-user access; OS + Postgres + Q-

Component	Spec	Approx. EUR	Why
			KYC API + ClamAV
Storage (primary)	1 TB NVMe SSD	80	Headroom for 50 clients × CDD docs over 5 yr
Storage (mirror)	1 TB NVMe SSD #2 (Windows Storage Spaces mirror)	80	RAID1 protects against single-disk failure
Storage (backup target)	4 TB NAS (Synology DS124 or DS224+)	350	Centralised office backup target
UPS	APC Smart-UPS C 1000VA (LCD, USB-management)	230	Smart-UPS line has the management daemon Q-KYC's auto-shutdown hook integrates with
Network	Office switch + business router with proper firewall (Mikrotik / Ubiquiti)	200	
Display	Two monitors for the MLRO + one each for compliance officers	240+	
Subtotal		**~2,180**	

Software — customer provides

Item	EUR/yr	Notes
Windows 11 Pro licence (if new)	one-off ~180	
Microsoft 365 Business Standard	144/user/yr	MLRO + officers
Endpoint AV (Windows Defender for Business / Bitdefender / Sophos)	optional, 30/user/yr	Defender alone is fine; commercial AV adds reporting

Backup architecture

Copy	Where	Frequency	Retention	EUR/yr

Copy	Where	Frequency	Retention	EUR/yr
1 — live	Workstation NVMe (mirrored)	continuous	5 yr	0
2 — NAS	Synology DS224+ in the same office	nightly + hourly snapshots	12 months	one-off 350
3 — off-site	Backblaze B2 or Synology C2	nightly	5 yr	~150-300

Power-continuity

- **UPS runtime target:** ≥ 30 minutes under load. Enough for the graceful shutdown daemon + headroom for typical SXM power outages (most resolve in 5-15 min).
- **Generator:** optional. A small portable inverter generator (Honda EU2200i or equiv., ~€1,500) covers outages that exceed UPS runtime; for a Tier-M firm, the off-site backup makes this less urgent — you can suspend operations and resume next day with data intact.
- **Total time from outage to safe state:** ≤ 5 minutes.

Disaster recovery

Metric	Target
RTO	< 2 hours (replacement workstation already imaged; NAS-restore from snapshot)
RPO	< 1 hour (hourly NAS snapshots)
Backup verification	nightly automated `verify_audit_chain.ps1`
Annual DR test	once per year, restore to a spare PC, verify chain

Total external CAPEX/OPEX for Tier M

Year 1	EUR
Hardware one-off	2,180
NAS + backup target setup	350 (included above)
Off-site backup (12 months)	250
Year-1 external total	**~2,430**
Yr 2-5 annual external	**~250/yr** (off-site backup + UPS battery replacement yr 3)

Tier L — Mid-size DNFBP / TCSP / 15-50 staff / 50-500 active clients

Profile: TCSP, mid-size accountancy, or a multi-partner notarial practice. Q-KYC runs on a small dedicated server in the office's IT cabinet. Multiple compliance officers + dedicated MLRO + audit-staff access. Often integrated with the firm's domain authentication.

Hardware — minimum

Component	Spec	Approx. EUR	Why
Server	Mini-tower server-grade — HPE ProLiant ML30 Gen11 / Dell PowerEdge T150 / Lenovo ThinkSystem ST50	1,400	Server-grade hardware = ECC RAM support, IPMI management, RAID controller
CPU	Xeon E-2400 series or Ryzen Pro	included	
RAM	64 GB DDR5 ECC	350	ECC mandatory — catches memory bit-flips that would corrupt the audit-chain hash mid-write
Storage (primary)	2× 2 TB NVMe enterprise SSD in RAID1	600	Mirror + enterprise endurance
Storage (backup local)	8 TB NAS — Synology DS923+ with 2× 8 TB HDD in SHR	1,200	Local off-server backup target
UPS	APC Smart-UPS SRT 2200VA online double-conversion	1,400	Online (true UPS) — power is always clean. Required for sensitive workloads.
Network	Managed switch + business firewall (Fortigate 40F or pfSense appliance)	800	Real firewall, not a consumer router
Out-of-band management	iDRAC / iLO licence	included	Remote console + power control for DR

Component	Spec	Approx. EUR	Why
Subtotal		**~5,750**	

Software — customer provides

Item	EUR/yr	Notes
Windows Server 2025 Standard (16-core)	one-off ~900	Or Linux + native PostgreSQL if customer prefers
Or Linux (Ubuntu Server LTS / Debian)	0	Equally supported by Q-KYC
AD-integration (Microsoft 365 Business Premium)	220/user/yr	For SSO into Q-KYC if desired
Backup software (Veeam Backup Community / Iperius)	one-off 600	Centralised backup management
Off-site backup (Backblaze B2 / Synology C2 / Azure Blob Cool)	~500-1,000/yr	Tier-L data volumes need real bandwidth

Backup architecture

Copy	Where	Frequency	Retention	EUR/yr
1 — live	Server NVMe RAID1	continuous	5 yr	0
2 — NAS	Synology DS923+ in adjacent room or fireproof safe	hourly snapshots	12 months	one-off 1,200
3 — off-site	Backblaze B2 / Azure Cool Blob	nightly	5 yr (NOIS art. 33)	~600-1,000
4 — warm-DR (optional)	Second server image at home office or secondary site	weekly sync	30 days	~1,500 one-off

Power-continuity — full HA path

- **UPS runtime target:** ≥ 60 minutes under load.

- **Generator: strongly recommended** at Tier L. Small standby diesel/petrol generator (3 kW class, ~€2,500-4,000) with automatic transfer switch. Covers extended SXM outages (hurricane prep).
- **Auto-shutdown daemon:** PowerChute Network Shutdown — talks to UPS over network, signals Windows / Linux at 80% battery depletion to begin shutdown. Q-KYC-API service stops cleanly; PostgreSQL flushes WAL; hash chain remains intact.
- **Total time from outage to safe state:** ≤ 30 seconds (UPS) + full graceful shutdown ≤ 3 minutes.

Disaster recovery

Metric	Target
RTO	< 1 hour (replacement server pre-imaged; NAS restore via 10 Gbps internal link)
RPO	< 1 hour (hourly NAS snapshot)
Hot-DR target (optional)	< 5 min RTO if warm-DR site online
Backup verification	nightly automated `verify_audit_chain.ps1` on the restored NAS image
Annual DR test	twice per year, including hurricane-season run-up (May & October)
Hurricane evacuation runbook	dedicated procedure: shutdown sequence, NAS removal, off-island data verification

Total external CAPEX/OPEX for Tier L

Year 1	EUR
Hardware one-off	5,750
Server OS licence	900
Backup software	600
Generator + transfer switch	3,500 (optional, recommended)
Off-site backup (12 mo)	800
Warm-DR setup (optional)	1,500 one-off
Year-1 external total	**~10,750** (or **~9,250** without warm-DR)
Yr 2-5 annual external	**~800-1,200/yr**

Comparison summary

The Q-KYC fee rows below are install + annual subscription. They are **separate** from the external hardware/backup costs above, which the firm carries regardless of which AML system it runs.

Item	Tier-1	Tier-2	Tier-3
Hardware CAPEX (Yr 1)	~€1,000	~€2,200	~€5,800
Off-site backup (Yr 1)	~€100	~€250	~€800
Generator (optional)	—	—	~€3,500
Total Yr 1 external	**~€1,100**	**~€2,450**	**~€9,000-11,000**
Total Yr 2-5 external OPEX	~€100/yr	~€250/yr	~€800-1,200/yr
Q-KYC list (Yr 1: install + annual)	€1,500 + €720	€2,500 + €2,400	€3,000 + €18,000
Q-KYC pilot (Yr 1: install + −25% annual)	€1,500 + €540	€2,500 + €1,800	€3,000 + €13,500

Q-KYC install excludes hardware and external subscriptions (e.g. cloud storage); the pilot −25% applies to the annual subscription only (first 10 subscribers, 3-year commitment).

For a CBCS supervisor: when asked "what is the total first-year cost of your AML compliance platform?", the answer for a Tier-2 firm is: ~€2,450 external hardware + €2,500 install + €1,800 pilot annual = **~€6,750 year 1**. The cloud-SaaS alternatives (ComplyAdvantage, Napier, Quantexa) are quote-priced — they publish no enterprise rates — and ship client data outside SXM.

Safe-shutdown procedure (all tiers)

Q-KYC's hash-chained audit log makes graceful shutdown a real requirement, not a nice-to-have. The procedure:

1. **UPS triggers** at 20% battery remaining (configurable).
2. **PowerChute / NUT daemon** sends shutdown signal to the OS.
3. **OS sends SIGTERM** to all running services including `Q-KYC-API` (managed by nssm on Windows / systemd on Linux).
4. **Q-KYC-API service** receives SIGTERM:
    - Stops accepting new HTTP requests
    - Allows in-flight requests up to 10 seconds to finish
    - Flushes any pending audit events to the database
    - Disconnects from PostgreSQL cleanly
5. **PostgreSQL** receives shutdown signal:

    - Completes any open transactions
    - Flushes WAL to disk
    - Closes the data files
6. **OS halts.**

Total time: typically < 60 seconds. UPS runtime must exceed this with margin.

If the UPS dies before this completes: - PostgreSQL's WAL design means the database recovers automatically on next boot — uncommitted transactions are rolled back; committed transactions are replayed from WAL - The audit chain stays mathematically intact: any event that wasn't yet committed never existed; events that WERE committed have correct previous-hash pointers - The `verify_audit_chain.ps1` after recovery confirms integrity

No customer action required during the outage. The system recovers on its own. The MLRO logs in after power restoration, verifies the chain, and continues work.

Quick recovery after a calamity

A "calamity" in SXM context is most commonly a hurricane (annual risk) or extended grid failure. The Q-KYC recovery procedure:

1. **Phase 0 — pre-calamity** (every September):
    - Verify backup integrity with `verify_audit_chain.ps1`
    - Confirm off-site backup is current
    - For Tier L: confirm warm-DR site is online
2. **Phase 1 — within 24h of calamity:**
    - Confirm hardware status (visit office or remote check)
    - If primary site is unreachable: trigger DR site (Tier L)
    - If primary hardware is destroyed: order replacement
3. **Phase 2 — within RTO target:**
    - Image replacement hardware with the standard Q-KYC install image
    - Restore the latest backup from off-site provider
    - Run `verify_audit_chain.ps1` — must show PASS before any new operations begin
    - Restore the firm's mail + portal access
    - Notify CBCS of operational status (within 48h is best practice)
4. **Phase 3 — within 7 days:**
    - Conduct a post-mortem: what worked, what didn't
    - Update the runbook
    - File any required incident report with CBCS / FIU

For Tier S, Phases 1-2 take ~4 hours. For Tier L with warm-DR, ~30 minutes.

What the customer should NOT do

- ❌ **Run Q-KYC on a laptop without dedicated backup.** Laptops get stolen, dropped, and battery-die at the worst times. NOIS art. 33 requires CDD records intact for 5 years — laptops are fragile.
- ❌ **Skip the UPS.** Power outages are routine in SXM. Without UPS every outage is a roll of the dice.
- ❌ **Skip the off-site backup.** Local backup alone fails the 3-2-1 rule. NOIS art. 33's "intact" interpretation depends on having a recoverable copy when the office is gone.
- ❌ **Run on Windows Home edition.** No BitLocker, no domain join, no proper service management. Pro is the floor.
- ❌ **Use spinning HDD for the primary storage.** PostgreSQL + ClamAV + concurrent screening writes will saturate spinning disk and cause user-visible latency. SSD is the floor.
- ❌ **Defer the UPS battery replacement.** UPS batteries die at ~3 years. Plan replacement at year 3 (~€60-200 depending on UPS class).

What we provide vs what the customer provides

Layer	Q-KYC SXM provides	Customer provides
Application	✓ Q-KYC binaries, schema, screening connectors	—
Database	✓ Bundled PostgreSQL 18, schema, migrations	—
OS	—	Windows 11 Pro / Server, or Linux LTS
Hardware	—	Per-tier specs above
Network	—	Office router + ISP
Power continuity	guidance + auto-shutdown hooks	UPS, generator (Tier L)
Backup software	sample scripts + verifier	Veeam / Iperius / pCloud / etc.
Off-site backup	guidance	subscription with EU-resident provider
Audit verifier	✓ `verify_audit_chain.ps1` ships with install	—

Layer	Q-KYC SXM provides	Customer provides
Disaster-recovery runbook	template + tested procedure	adaptation to their specific premises
Annual DR test	✓ we run it with the customer once/year (pilot phase)	host the test
Support during incident	✓ pilot phase: free regulator-meeting support, 4-hour response on outage	mail / phone access to MLRO

Compliance citations (for the customer's procurement file)

When IT procurement asks "why are we spending €11,000 on a Q-KYC deployment?" the customer can cite:

- **NOIS art. 33** — 5-year retention; intact records
- **LBP art. 14** — appropriate security measures; data integrity
- **CBCS P&G §6** — DNFBP operational-risk management
- **CBCS P&G §9** — business-continuity planning required
- **2022 CFATF Mutual Evaluation Report on the Kingdom** — recommendation 17 (DNFBP supervision improvement) implicitly requires firms to have documented controls

For a procurement audit, this document IS the documented control.