NIS2 ARTICLE 21(2) EVIDENCE REPORT

Certificate Lifecycle and Renewal Controls

PREPARED BY **SkyQon Digital Trust Center**

PREPARED FOR **SkyQon Internal Lab**

OVERALL EVIDENCE SCORE

76 /100

↑ 10 vs prior period (2026-06-13)

Monitoring continuity	100	= 0
Cryptographic posture	45	= 0
Responsiveness	47	↑ 47
Renewal control	100	= 0

REPORT METADATA

REGULATORY FRAMEWORK	NIS2 Directive (EU) 2022/2555 · Article 21(2)
METHODOLOGY	Documented in this report (Methodology section)
OBSERVATION PERIOD	2026-06-01 → 2026-07-01
TENANT IDENTIFIER	`skyqon-internal`
REPORT IDENTIFIER	`1620e0eb-7356-4436-b70f-2200c9deba0c`
GENERATION TIMESTAMP	2026-07-02T11:31:14Z
EVIDENCE HASH	`sha256:0426f6e7909d…`
DOCUMENT VERSION	1.0 · Final
DISTRIBUTION	For exclusive use of SkyQon Internal Lab — not for redistribution.

EXECUTIVE SUMMARY

Overall evidence score

Composite of four sub-scores — monitoring continuity, renewal control, alert responsiveness, and cryptographic posture — derived from this report's observation window.

76 / 100

Monitoring continuity	100	w=25%
Cryptographic posture	45	w=25%
Responsiveness	47	w=20%
Renewal control	100	w=30%

NIS2 Article 21(2) coverage at a glance

●	Art. 21(2)(f)	Policies to assess the effectiveness of risk-management measures	direct
●	Art. 21(2)(i)	Cryptography and, where appropriate, encryption policies	direct
●	Art. 21(2)(g)	Basic cyber hygiene practices	supporting
●	Art. 21(2)(e)	Security in network/information-systems maintenance, including vulnerability handling	supporting
●	Art. 21(2)(a)	Risk analysis and information-system security policies	input-only — NOT claimed as covered

Top findings

1. 8 alert(s) remained open at the end of the observation period.
2. Post-quantum readiness is low — 0/10 endpoints use PQ-ready or hybrid-capable signatures.

> This report presents evidence that supports an audit of certain NIS2 Article 21(2) risk-management measures relating to certificate lifecycle and cryptographic posture. It does NOT constitute compliance, certification, or a legal attestation of NIS2 conformity. The tenant remains responsible for its own compliance determination.

METHODOLOGY

How this report is derived

Transparency about scope, data sources, and the scoring rubric. An auditor should be able to reproduce every number on the cover from the underlying evidence payload.

Data sources

- **External TLS scans** — periodic outbound TLS handshakes from SkyQon Digital Trust Center to each declared (host, port). One scan_runs row per attempt; success or error is captured.
- **Certificate inventory** — append-only observations (one certificates row per (host, port, scan)); the latest row per endpoint represents the current state.
- **Alerts ledger** — emitted notifications with created_at / notified_at / resolved_at timestamps.
- **Renewals** — derived from successive certificate observations on the same (host, port) where not_after changed; surfaced via the v_renewal_events view.

Scoring rubric

SUB-SCORE	FORMULA	WEIGHT
Monitoring continuity	`scans_complete / scans_total` (0 if no scans ran in the period — a coverage gap is itself negative evidence)	25%
Renewal control	`renewed_early / renewals_total` where a renewal is early if observed before the prior `not_after` (100 if no renewals were due)	30%
Responsiveness	`alerts_resolved / alerts_total` over non-suppressed alerts (100 if none fired)	20%
Cryptographic posture	`mean(security_score)` over the latest certificate per (host, port) at `period_end`	25%
Overall	Weighted arithmetic mean of the four sub-scores. Each sub-score is 0–100; higher is better.	—

What's covered, what's supporting, what's NOT covered

The NIS2 Art. 21(2) mapping later in this report classifies coverage as:

- **direct** — this report contains the primary evidence for the measure.
- **supporting** — this report contains useful but secondary evidence; the primary control lives elsewhere.
- **input-only — NOT claimed as covered** — this report does *not* establish compliance with the measure; we list it only to be explicit about scope.

An honest deliverable: certificate-lifecycle monitoring evidences part of Art. 21, not all of it. Measures around supply-chain risk, incident response, business continuity, and personnel security require other controls.

Integrity model

The underlying evidence payload (summary_json) is serialised with sorted keys and no whitespace, then hashed with SHA-256. The hash printed in this report's footer and on the final page is computed over the *evidence*, not over the rendered PDF — so a re-rendered PDF of the same evidence has the same hash.

01

SECTION 1

Monitoring continuity

Did SkyQon Digital Trust Center actually scan the declared endpoints during the observation period? Gaps here are negative evidence — even a perfect inventory snapshot is unreliable if we stopped looking.

SCANS RUN	COMPLETED	FAILED	COVERAGE	FIRST SCAN	LAST SCAN
1649	1648	0	100%	2026-06-01T00:07	2026-06-30T22:55

SECTION 2

Inventory snapshot — 10 endpoints

Latest leaf certificate observed per (host, port) at the end of the observation period. Risk is the scanner's classification at scan time; PQ status is the post-quantum readiness of the signature/key algorithm.

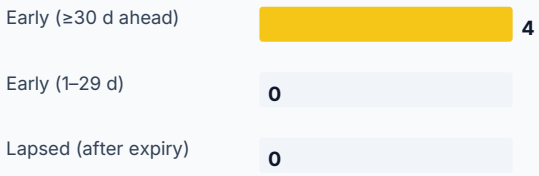
HOST	PORT	ISSUER	EXPIRES	DAYS	RISK	PQ	SCORE
dashboard.skyqon.com	443	YE2	2026-09-02	64	WARNING	LEGACY	90
dashboard.skyqon.com	8443	YE2	2026-09-02	64	WARNING	LEGACY	90
keycloak.skyqon.com	443	—	–	0	UNKNOWN	LEGACY	0
keycloak.skyqon.com	8443	—	–	0	UNKNOWN	LEGACY	0
nc.skyqon.com	443	R13	2026-08-16	52	WARNING	LEGACY	90
nc.skyqon.com	8443	—	–	0	UNKNOWN	LEGACY	0
pki.skyqon.com	443	—	–	0	UNKNOWN	LEGACY	0
pki.skyqon.com	8443	—	–	0	UNKNOWN	LEGACY	0
skyqon.com	443	YE2	2026-09-02	64	WARNING	LEGACY	90
skyqon.com	8443	YE2	2026-09-02	64	WARNING	LEGACY	90

SECTION 3

Proof of renewal control

4 renewal event(s) observed — 4 early, 0 lapsed. An "early" renewal is one observed before the prior certificate had expired; a "lapse" means the new certificate is itself already expired at observation time.

DISTRIBUTION OF RENEWAL GAPS



HOST	PORT	OBSERVED	OLD EXPIRY	NEW EXPIRY	GAP (DAYS)	EARLY?
dashboard.skyqon.com	443	2026-06-05	2026-07-05	2026-09-02	-30.89	yes
dashboard.skyqon.com	8443	2026-06-05	2026-07-05	2026-09-02	-30.89	yes
skyqon.com	443	2026-06-05	2026-07-05	2026-09-02	-30.89	yes
skyqon.com	8443	2026-06-05	2026-07-05	2026-09-02	-30.89	yes

SECTION 4

Control-effectiveness ledger

27 alert(s) emitted — 7 resolved, 8 open. Resolution is the auditable evidence that detection led to action.

TYPE	SEVERITY	CREATED	NOTIFIED	RESOLVED
EXPIRY_WARNING	WARNING	2026-06-09T18:59	2026-06-09T18:59	OPEN
EXPIRY_WARNING	WARNING	2026-06-09T18:59	2026-06-09T18:59	OPEN
EXPIRY_WARNING	WARNING	2026-06-09T18:59	2026-06-09T18:59	OPEN
EXPIRY_WARNING	WARNING	2026-06-09T18:59	2026-06-09T18:59	OPEN
EXPIRY_WARNING	WARNING	2026-06-09T18:59	2026-06-09T18:59	OPEN
UNEXPECTED_CA	CRITICAL	2026-06-13T11:09	2026-06-13T11:09	OPEN
EXPIRY_WARNING	WARNING	2026-06-18T10:21	2026-06-18T10:21	OPEN
EXPIRY_WARNING	WARNING	2026-06-18T10:21	2026-06-18T10:21	OPEN
EXPIRY_WARNING	WARNING	2026-06-18T10:21	2026-06-18T10:21	OPEN
DOMAIN_TRANSFER_UNLOCKED	WARNING	2026-06-18T17:55	—	2026-06-19T20:38
EXPIRY_WARNING	WARNING	2026-06-18T18:16	2026-06-18T18:16	OPEN
EXPIRY_WARNING	WARNING	2026-06-18T18:16	2026-06-18T18:16	OPEN
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-19T09:40	2026-06-19T09:40	OPEN
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-19T09:40	2026-06-19T09:40	OPEN
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-19T09:40	2026-06-19T09:40	OPEN
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-19T09:40	2026-06-19T09:40	OPEN
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-19T09:40	2026-06-19T09:40	OPEN
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-20T09:58	2026-06-20T09:58	2026-06-24T15:32
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-20T09:58	2026-06-20T09:58	2026-06-24T15:32
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-20T09:58	2026-06-20T09:58	2026-06-24T15:32
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-20T09:58	2026-06-20T09:58	2026-06-24T14:31
DMARC_POLICY_TOO_WEAK	WARNING	2026-06-20T09:58	2026-06-20T09:58	2026-06-24T14:31
MTA_STS_NOT_ENFORCING	WARNING	2026-06-20T23:47	2026-06-21T17:01	OPEN
PQC_REGRESSION	WARNING	2026-06-24T10:49	—	OPEN
ATTACK_SURFACE_SHADOW_HOST	WARNING	2026-06-25T09:34	2026-06-25T09:34	2026-06-26T09:46
ATTACK_SURFACE_SHADOW_HOST	WARNING	2026-06-25T09:34	2026-06-25T09:34	2026-06-26T09:45

MTA_STS_NOT_ENFORCING	WARNING	2026-06-25T17:22	2026-06-25T17:22	OPEN

05

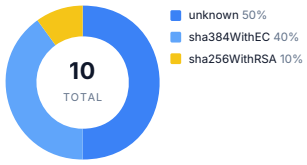
SECTION 5

Cryptographic posture

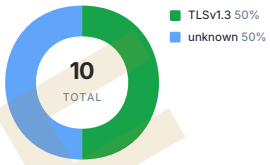
Distribution across the inventory at period_end. The PQ column tracks readiness against NIST FIPS 203 / 204 / 205 (Kyber, Dilithium, SPHINCS+); most production deployments today still appear as NOT_READY.

PQ READINESS

SIGNATURE ALGORITHMS



TLS VERSIONS



Cryptographic asset inventory

Consolidated, de-duplicated register of every cryptographic identity — scanned certificates, auto-renewed certificates, discovered hosts and non-TLS assets — as of report generation.

IDENTITIES	AUTO-RENEWED	INTERNAL-CA	EXPIRING < 30 DAYS	QUANTUM-VULNERABLE
2	0	0	0	2

06

SECTION 6

NIS2 Article 21(2) — evidence mapping

The honest map: for each sub-clause of Art. 21(2), what evidence (if any) this report contributes. Sub-clauses we do not cover are listed explicitly so a reader can see the scope boundary.

MEASURE	TITLE	EVIDENCE	COVERAGE
21(2)(f)	Policies to assess the effectiveness of risk-management measures	Control-effectiveness ledger (§5) + renewal-control proof	direct
21(2)(i)	Cryptography and, where appropriate, encryption policies	Cryptographic posture: algorithms, key sizes, TLS versions, post-quantum readiness, weak-algorithm exceptions over time	direct
21(2)(g)	Basic cyber hygiene practices	Monitoring continuity + demonstrated timely certificate renewal	supporting
21(2)(e)	Security in network/information-systems maintenance, including vulnerability handling	Exceptions ledger — detection-to-resolution of expiring/weak certs	supporting
21(2)(a)	Risk analysis and information-system security policies	Inventory + posture feed the tenant's own risk analysis only	input-only — NOT claimed as covered

INTEGRITY VERIFICATION

Verify this report

The evidence underneath this PDF is hashed with SHA-256. Anyone with a copy of this report can confirm — via the SkyQon API — that the evidence payload was not altered after the report was generated.

Scan the QR or visit:

```
https://dashboard.skyqon.com/v1/compliance/skyqon-internal/reports/
1620e0eb-7356-4436-b70f-2200c9deba0c/verify
```

Evidence hash

`sha256:0426f6e7909db4412654b982bc0382f01c5df420eafe7bff938bb0d299458e4a`

How verification works

1. The verification endpoint reads the stored summary_json (the evidence source of truth) for this report.
2. It re-runs the canonical serialisation (sorted keys, no whitespace) and re-computes SHA-256 over the result.
3. If the re-computed hash matches the hash printed above, the evidence has not been altered since report generation.

PDF rendering is deterministic from the evidence: regenerating this PDF produces a byte-identical hash on this page (different layout dates aside).

Generated by SkyQon Digital Trust Center · skyqon.com · hello@skyqon.com
Report version 1.0 · Tenant skyqon-internal · Plan business