SAMPLE: Quantum-Safe Readiness Check, one whole labelled sample report (EN)

> **SAMPLE. Not a client's report.** Every section below is a labelled sample and keeps its own label. The sections come from three different sources (a fictional client's sample pack, a real probe of Adwaizer's own domains, and made-up test fixtures); they are not one engagement. Not a certification, an audit opinion or legal advice, and it does not guarantee quantum safety.

#	Section of the delivered report	In this sample	Source file
1	Cover: readiness grade, summary, verification period; Scope (`:115` - `:153`)	not in this sample	none
2	Attestation letter (`:155`)	not in this sample	none
3	Applicable clauses and answers (`:159`)	yes	`qsafe examples/sample-pack/answer-sheet-en.md @ f662b0d`
4	Verified cryptographic profile: endpoints (`:171` - `:182`)	yes, with the CBOM	`2026-10-30-sample-endpoint-section.md`
4	Verified cryptographic profile: cryptographic modules (`:183` - `:193`)	not in this sample	none
5	Gaps and remediation plan (`:196`)	not in this sample	none
6	Crypto-agility statement (`:206`)	not in this sample	none
7	Upstream providers (`:220`); Decisions on record (`:212`) when recorded	not in this sample	none
8	Methodology and limitations (`:228`)	not in this sample	none
9	Signatures and Verification (`:240` , `:246`)	not in this sample	none
Appendix	SPIN 6.2.3 application portfolio (APM) fields (`:257` , only when the clause is in scope)	not in this sample	none
Annex	Mail in transit (free snapshot, `snapshot_show.html:31` - `:45`)	yes	`2026-10-30-sample-mail-transit-section.md`

---

1. Readiness grade, summary, verification period and scope

`not in this sample`

2. Attestation

```
not in this sample
```

3. Applicable clauses and answers

Labelled sample: Northbridge Software Inc. and its product are fictional; the pack's endpoints were Adwaizer's own domains standing in for a client's, probed on 18 Oct 2026; the pack was issued on 26 Oct 2026, so its endpoint rows predate the 30 Oct probe in section 4.

ADW-QSR-SAMPLE-002 · 2026-10-26 · grade C

Second reviewer: not yet appointed

Clause	Source	Status	Response	Evidence
CA-SPIN-6.3.1	SPIN, section 6.3.1 (procurement clauses)	Committed (2026-12-31)	Not met today; committed by the client to be met by 2026-12-31 (client representation, verified by Adwaizer on that date).	Key establishment hybrid today; signatures by 15 Dec 2026; FIPS 140-3 module migration by 31 Dec 2026
CA-ITSM00501-2.1.1-KE	ITSM.00.501, section 2.1.1 (recommended cryptographic algorithms)	Compliant (measured)	Compliant, measured on the deployed estate; see evidence.	adwaizer.com:443: X25519MLKEM768; www.adwaizer.com:443: X25519MLKEM768
CA-ITSM00501-2.1.1-DS	ITSM.00.501, section 2.1.1 (recommended cryptographic algorithms)	Committed (2026-12-15)	Not met today; committed by the client to be met by 2026-12-15 (client representation, verified by Adwaizer on that date).	Vendor roadmap: ML-DSA-65 code signing in release 4.2 (Q4 2026)
CA-ITSM00501-2.1.2	ITSM.00.501, section 2.1.2 (cryptographic agility)	Compliant (attested)	Compliant on the client's evidence (document or interview), not measured by Adwaizer; see evidence.	Cipher suites, groups and key sizes configurable in the edge policy; application signing algorithm selectable per environment; updates signed with Cosign
CA-ITSM00501-2.1.3	ITSM.00.501, sections 2.1.3 and 2.2.3 (cryptographic certification)	Gap	Not yet compliant; remediation planned (see gaps).	OpenSSL FIPS Provider 3.0.8 (application TLS): CMVP #4282 FIPS 140-2 Historical; Seagate SSG5 SED (storage encryption): CMVP #5552 FIPS 140-3 Active; Vendor HSM (key wrapping): CMVP certificate pending
CA-ITSM00501-2.2	ITSM.00.501, section 2.2 (service providers and cloud services)	Gap	Not yet compliant; remediation planned (see gaps).	adwaizer.com:443: versions TLSv1/TLSv1.1/TLSv1.2/TLSv1.3; www.adwaizer.com:443: versions TLSv1/TLSv1.1/TLSv1.2/TLSv1.3

Clause	Source	Status	Response	Evidence
CA-SSC-CSIAAS2024-CP	CS-IAAS-2024, Cryptographic Protection, clauses (1) to (7)	Committed (2026-12-31)	Not met today; committed by the client to be met by 2026-12-31 (client representation, verified by Adwaizer on that date).	Clause (5) active CMVP certification: see modules; (3) and (7) configurable algorithms and agility: see crypto-agility statement
CA-SPIN-6.2.3	SPIN, section 6.2.3 (application portfolio records)	Compliant (attested)	Compliant on the client's evidence (document or interview), not measured by Adwaizer; see evidence.	APM record fields supplied in the appendix: components, algorithms, hosting, dependencies, versions, contract expiry 2028-03-31, refresh 2027, contact, priority High
AU-ASD-VENDORQ	ASD vendor questions (16 Jul 2026) and AUSCERT questionnaire v1.0 (Aug 2026)	Compliant (attested)	Compliant on the client's evidence (document or interview), not measured by Adwaizer; see evidence.	Board-approved quantum readiness plan (Sep 2026); CBOM available on request; no SHA-1 or 3DES in the service chain

4. Verified cryptographic profile

Shown to the prospect:

> **Labelled sample.** This is a real run of the Quantum-Safe endpoint probe and CBOM merge, on two domains Adwaizer owns: adwaizer.com and acuarela.adwaizer.com. It is not a client's report. Run on 30 Oct 2026 at 11:46 UTC (probe time), on Adwaizer's Mac with OpenSSL 3.6.4 and a direct TLS connection (no proxy), from adwaizer-qsafe-pipeline at commit `f662b0d`.

Endpoint profile

Host	Grade	Key exchange (default)	TLS versions	Leaf key	Findings
adwaizer.com:443	A	hybrid X25519MLKEM768, TLSv1.3, TLS_AES_256_GCM_SHA384	TLSv1.3 and TLSv1.2 yes; TLSv1 and TLSv1.1 no	EC-256 (secp256r1), signed ecdsa-with-SHA384 by Let's Encrypt YE1	**low** `cert-classical-key` (clause CA-ITSM00501-2.1.1-DS)

Host	Grade	Key exchange (default)	TLS versions	Leaf key	Findings
acuarela.adwaizer.com:443	A	hybrid X25519MLKEM768, TLSv1.3, TLS_AES_256_GCM_SHA384	TLSv1.3 and TLSv1.2 yes; TLSv1 and TLSv1.1 no	EC-256 (secp256r1), signed ecdsa-with-SHA384 by Let's Encrypt YE1	**low** `cert-classical-key` (clause CA-ITSM00501-2.1.1-DS)

Both hosts present the same leaf certificate (`CN=adwaizer.com`, names `*.adwaizer.com` and `adwaizer.com`, SHA-256 `29a60d45…64fa`), valid until 24 Jan 2027 (85 days left at the run), with a four-certificate chain up to ISRG Root X1.

Cryptographic bill of materials (CBOM)

2 CBOMs (one per host) merged into 7 components, valid CycloneDX 1.6: the X25519MLKEM768 key exchange (key agreement, NIST quantum security level 3), one TLSv1.3 protocol entry per host, and the four certificates of the shared chain.

What the findings mean for you

- **Hybrid key exchange X25519MLKEM768 on both hosts.** Traffic to these sites is already encrypted with a key exchange that combines a classical and a post-quantum (ML-KEM) method, which is designed so that traffic recorded today cannot later be decrypted by a quantum computer. Nothing is needed here except keeping it on.
- **[low]** `cert-classical-key` **on both hosts.** The certificate that proves the sites' identity still uses a classical EC-256 key, which a large future quantum computer could in principle forge; this is about impersonation later, not about reading today's traffic. The probe's advice is to "plan ML-DSA certificates as the CA adds support", so the action is a dated plan with the certificate authority, not an emergency fix.

This sample is not a certification, an audit opinion or legal advice, and it does not guarantee quantum safety.

Cryptographic modules

```
not in this sample
```

5. Gaps and remediation plan

```
not in this sample
```

6. Crypto-agility statement

```
not in this sample
```

7. Upstream providers

```
not in this sample
```

8. Methodology and limitations

not in this sample

9. Signatures and verification

not in this sample

Appendix: SPIN 6.2.3 application portfolio (APM) fields

not in this sample

Annex: Mail in transit (free snapshot)

Not a section of the delivered attestation: it is what the free snapshot page shows.

Sample from test fixtures. Every value below comes from the made-up domain `example.ca` in the pipeline's committed tests. No real domain was looked up, and nothing was published or sent.

What the check reads

DNS records of the buyer's own domain, read-only. It never connects to the mail servers on port 25 and never fetches the MTA-STS policy file (`src/qsafe/ingest/dns.py:91-:93`; `tests/test_mail_transport.py:48-:49`). The page's own line for buyers: "Whether mail sent to you is protected on its way, read from your public DNS only." (`src/qsafe/web/i18n.py:109`).

Sample A: all four published

Fixture `ALL` (`tests/test_mail_transport.py:25-:31`), asserted by `test_all_four_present` (`:34-:39`).

Check	Page shows	What it means for a buyer	Cite (qsafe @ f662b0d)
MX	present `10 mx1.example.ca` `20 mx2.example.ca`	The domain names two mail servers, listed by preference. These are the hosts the other three checks are about. A null MX (`0 .`, "this domain takes no mail") counts as no host.	`src/qsafe/ingest/dns.py:95-:101`; `tests/test_mail_transport.py:36`, `:64-:68`; `src/qsafe/web/templates/snapshot_show.html:39`

Check	Page shows	What it means for a buyer	Cite (qsafe @ f662b0d)
MTA-STS	present `id=20261027T000000`	The domain publishes the `_mta-sts` TXT record that tells sending servers a TLS policy exists. Only the record is read. Whether the policy file says `enforce` or `testing` is not checked by the snapshot.	`src/qsafe/ingest/dns.py:102, :107; tests/test_mail_transport.py:37; src/qsafe/web/templates/snapshot_show.html:40`
TLS-RPT	present `mailto:tlsrpt@example.ca`	The domain asks sending servers to report TLS failures, and the page shows where those reports go. Without it, failed encrypted delivery goes unseen.	`src/qsafe/ingest/dns.py:103, :108; tests/test_mail_transport.py:38; src/qsafe/web/templates/snapshot_show.html:41`
DANE	present `mx1.example.ca (2 TLSA) mx2.example.ca (1 TLSA)`	Each mail server publishes TLSA records, which pin its certificate in DNS, and the page counts them per server. The snapshot counts TLSA records only. It does not validate DNSSEC, which DANE relies on.	`src/qsafe/ingest/dns.py:104, :109; tests/test_mail_transport.py:39; src/qsafe/web/templates/snapshot_show.html:42`

Sample B: partly published

Fixture `ALL`, changed as two tests do: the `_mta-sts` TXT lacks `v=STSv1` (`test_mta_sts_txt_without_version_is_missing`, `tests/test_mail_transport.py:52-:55`), and `mx2` has no TLSA (`test_one_of_two_mx_hosts_with_tlsa`, `:58-:61`).

Check	Page shows	What it means for a buyer	Cite (qsafe @ f662b0d)
MX	present `10 mx1.example.ca 20 mx2.example.ca`	Same two mail servers as in A.	`src/qsafe/ingest/dns.py:95-:101`; `src/qsafe/web/templates/snapshot_show.html:39`
MTA-STS	missing	A TXT record without the `v=STSv1` version tag is not an MTA-STS record, so sending servers would ignore it, and the page says missing.	`src/qsafe/ingest/dns.py:42-:46, :102`; `tests/test_mail_transport.py:54`
TLS-RPT	present `mailto:tlsrpt@example.ca`	Reporting still works on its own.	`tests/test_mail_transport.py:55`; `src/qsafe/web/templates/snapshot_show.html:41`
DANE	present `mx1.example.ca (2 TLSA)`	DANE reads "present" as soon as one server has TLSA. The page lists only the servers that have it, so `mx2.example.ca` is uncovered and shows only by its absence from the list. Mail routed through `mx2` gets no DANE pin.	`src/qsafe/ingest/dns.py:104, :109`; `tests/test_mail_transport.py:61`; `src/qsafe/web/templates/snapshot_show.html:42` (`if n`)

Sample C: nothing published, or DNS unreadable

Case	Page shows	What it means for a buyer	Cite (qsafe @ f662b0d)
Nothing published (fixture `{}`)	MX missing · MTA-STS missing · TLS-RPT missing · DANE missing	No mail server is named, so there are no TLSA lookups either. A buyer whose mail runs on another domain sees this for the domain it entered.	`tests/test_mail_transport.py:42-:49`; `src/qsafe/web/templates/snapshot_show.html:37, :39-:42`
Resolver error (`SERVFAIL`)	"Your mail DNS records could not be read: SERVFAIL"	A DNS failure is shown as such. It never fails the snapshot or its TLS grades.	`src/qsafe/web/app.py:270-:273`; `tests/test_mail_transport.py:77-:86`; `src/qsafe/web/i18n.py:113`

What the section does not say

- It gives no grade and no pass or fail for mail. It shows present or missing per record (`src/qsafe/web/templates/snapshot_show.html:37`).
- It reads DNS only. It does not test that a mail server actually offers TLS on port 25, and it does not read the MTA-STS policy mode (`src/qsafe/ingest/dns.py:92-:93`).
- It says nothing about post-quantum key exchange for mail. The snapshot's hybrid key exchange grade is for the HTTPS endpoints above it on the page (`src/qsafe/web/i18n.py:106`).

SAMPLE. Not a client's report. Not a certification, an audit opinion or legal advice, and it does not guarantee quantum safety.