QScout HNDL Risk Scoring Methodology

Version 2.0 | February 2026

Document Classification: Public

Executive Summary

This document specifies the complete methodology used by QScout to calculate Harvest Now, Decrypt Later (HNDL) risk scores. The HNDL score quantifies an organization's exposure to the threat of adversaries collecting encrypted data today with the intent to decrypt it when cryptographically-relevant quantum computers (CRQCs) become available.

Key Properties of This Methodology:

- **7 weighted factors** producing a composite score from 0 to 100
- **Single break year calculation** producing a confidence interval, not a point estimate
- **Single migration deadline formula** derived deterministically from the break year interval
- **Full traceability** from scan data to final score, auditable at every step
- **Explicit CNSA 2.0 alignment** with NSA timeline requirements
- **No unsourced claims** -- all external references are cited with URLs and dates

This document is the **single source of truth**. Any discrepancy between this document, the backend implementation, the frontend calculator, or generated reports constitutes a defect that

> must be resolved in favor of this specification.

Revision History

Version	Date	Changes
2.0	February 2026	7-factor model, unified break year calculation, CNSA 2.0 alignment, confidence intervals, frontend calculator alignment, validation framework
1.0	February 2026	Initial 6-factor publication (superseded)

1. The HNDL Threat Model

1.1 Definition

Harvest Now, Decrypt Later (HNDL) is an attack strategy where adversaries:

1. Intercept and store encrypted network traffic today
2. Wait for quantum computers capable of breaking current encryption
3. Decrypt the harvested data retroactively

1.2 Why HNDL Matters

- **Data has a shelf life:** Financial records, healthcare data, and government secrets remain sensitive for decades
- **Quantum timeline uncertainty:** External CRQC timing estimates vary widely; Qtonic Quantum treats 2029 as a readiness/control planning date
- **Nation-state capability:** Well-resourced adversaries are already harvesting encrypted traffic (documented by NSA, CISA, and allied intelligence agencies)
- **Compliance drivers:** NIST PQC standards, NIST IR 8547 initial-public-draft transition planning, NSA CNSA 2.0 guidance for National Security Systems, OMB M-23-02, and Executive Order 14028 shape PQC readiness programs

- **Irreversibility:** Unlike most security incidents, HNDL exploitation cannot be remediated after the fact -- once data is harvested, it remains vulnerable regardless of future encryption upgrades

1.3 Vulnerable Algorithms

Algorithm	Type	Quantum Vulnerability	Break Mechanism
RSA-2048/4096	Key Exchange / Signature	**Broken** by Shor's algorithm	Polynomial-time integer factorization
ECDSA P-256/P-384	Digital Signature	**Broken** by Shor's algorithm	Elliptic curve discrete logarithm
ECDH	Key Agreement	**Broken** by Shor's algorithm	Elliptic curve discrete logarithm
DH (Diffie-Hellman)	Key Exchange	**Broken** by Shor's algorithm	Discrete logarithm problem
AES-128	Symmetric	**Weakened** by Grover's algorithm	Effective key space reduced to 64-bit
AES-256	Symmetric	**Reduced** to 128-bit equivalent	Still considered secure post-quantum
SHA-256	Hash	**Reduced** by Grover's algorithm	Collision resistance reduced from 128 to ~85 bits
ML-KEM (FIPS 203)	Key Encapsulation	**Quantum-safe**	Lattice-based, no known quantum speedup
ML-DSA (FIPS 204)	Digital Signature	**Quantum-safe**	Lattice-based, no known quantum speedup
SLH-DSA (FIPS 205)	Digital Signature	**Quantum-safe**	Hash-based, no known quantum speedup

2. HNDL Risk Score Calculation

2.1 Score Range and Risk Levels

The HNDL Risk Score is expressed as a value from **0 to 100**:

Score Range	Risk Level	Interpretation	Recommended Action Timeline
80-100	**CRITICAL**	Immediate action required	Begin PQC migration within 30 days
60-79	**HIGH**	Begin migration planning now	Complete assessment within 90 days
40-59	**MEDIUM**	Include in 12-month roadmap	Inventory and prioritize within 6 months
20-39	**LOW**	Monitor and reassess annually	Annual reassessment, maintain crypto-agility
0-19	**MINIMAL**	Current posture acceptable	Continue monitoring quantum developments

2.2 Scoring Formula

```
HNDL_Score = min(100, Sigma(Factor_i_Weight * Factor_i_Score_Normalized))
```

Where each factor score is first computed on a raw 0-10 scale, then normalized:

```
Factor_i_Score_Normalized = (Factor_i_Raw / 10) * 100
```

And the weighted sum produces the final 0-100 composite:

```
HNDL_Score = sum of (Weight_i * Factor_i_Score_Normalized) for all 7 factors
```

2.3 The Seven Factors

#	Factor	Weight	Source	Rationale for Weight
1	Data Sensitivity	25%	User input or industry default	Highest weight: determines the *value* of what an adversary can decrypt. Sensitive data drives the entire HNDL economic model.
2	Future Decrypt Risk	20%	Scan-derived (algorithm inventory)	Measures *how vulnerable* current cryptography is to quantum attack. Shor-vulnerable algorithms create the precondition for HNDL.

3	Adversary Capability	20%	User input or industry default	Measures *who* is likely to harvest data. Nation-state actors with storage infrastructure represent categorically different threat than opportunistic attackers.
4	Timeline Proximity	15%	Computed from GRI data + scenario	Measures *when* the threat materializes. Closer CRQC timelines increase urgency exponentially, but we weight this below data sensitivity because even distant threats matter for long-lived data.
5	Active Targeting Profile	10%	Scan-derived + industry context	Measures whether the organization is a *likely target* for data harvesting based on sector, geopolitical exposure, and observed adversary interest.
6	Present Crypto Hygiene	5%	Scan-derived (TLS config, headers, protocols)	Measures current classical security posture. Low weight because even perfect classical hygiene does not mitigate quantum threat, but poor hygiene compounds it.
7	Data Retention Window	5%	User input or regulatory default	Measures how long data must remain confidential. Low weight because it overlaps with Data Sensitivity, but explicit inclusion ensures organizations with unusually long retention periods are flagged.

Weight Justification Summary:

The weights reflect a risk model where *what* is at risk (Data Sensitivity, 25%) and *how breakable* it is (Future Decrypt Risk, 20%) together account for 45% of the score. *Who* would attack (Adversary Capability, 20%) accounts for 20% because HNDL is primarily a nation-state and APT concern. *When* the break happens (Timeline Proximity, 15%) and *whether* the org is targeted (Active Targeting, 10%) drive urgency. Classical hygiene (5%) and retention window (5%) are minor adjustments that prevent edge-case blindness.

These weights were designed to ensure that:

- An organization with Top Secret data and RSA-2048 always scores CRITICAL regardless of other factors
- An organization with public data never scores above LOW regardless of cryptographic posture
- Nation-state targeting elevates any MEDIUM score toward HIGH

3. Factor Definitions and Scoring

3.1 Factor 1: Data Sensitivity (Weight: 25%)

Definition: The classification level and regulatory significance of data protected by the assessed cryptographic infrastructure.

Measurement: User-provided during assessment intake, or derived from industry defaults for operator-reviewed QScout public-intake checks.

Score Scale (0-10):

Score	Classification	Examples	Regulatory Context
10	Top Secret / SAP	Classified national security data, nuclear command and control	ITAR, EAR, classified networks
8	Secret / Restricted	Government sensitive but unclassified, defense contractor CUI	CMMC Level 3, NIST 800-171
7	PII + Financial	SSN, credit card numbers, bank account details, tax records	PCI DSS, GLBA, SOX
6	PHI (Healthcare)	Medical records, genomic data, prescription history	HIPAA, HITECH, 42 CFR Part 2
5	Business Confidential	Trade secrets, M&A data, unreleased product plans	Trade secret law, NDA-protected
4	Professional Privileged	Attorney-client communications, audit workpapers	ABA Model Rules, PCAOB
3	Internal Only	Employee directories, internal memos, non-public policies	General corporate governance
2	Semi-public	Press releases before publication, non-material internal data	Minimal regulatory exposure
0	Public	Already-disclosed information, published documents	No confidentiality requirement

Industry Defaults (QScout public-intake estimate):

When user input is unavailable, the following defaults are applied based on detected or stated industry:

Industry	Default Score	Justification
Federal / Defense	8	Assumes CUI minimum; actual classified data raises to 10
Financial Services	7	PCI and GLBA data presumed
Healthcare	6	PHI presumed under HIPAA
Critical Infrastructure	6	NERC CIP data, OT telemetry
Legal / Professional Services	5	Privileged communications
Technology / SaaS	4	Customer data, source code
Retail / E-commerce	4	PCI cardholder data
General / Unknown	4	Conservative mid-range default

3.2 Factor 2: Future Decrypt Risk (Weight: 20%)

Definition: The degree to which currently deployed cryptographic algorithms are vulnerable to quantum attack via Shor's algorithm, Grover's algorithm, or other known quantum speedups.

Measurement: Directly derived from scan data. QScout inspects TLS handshakes, certificate chains, and protocol configurations to identify algorithms in use.

Score Scale (0-10):

Score	Cryptographic Configuration	Rationale
10	RSA-1024 only	Classically weak AND fully Shor-vulnerable. Already deprecated by NIST.
9	RSA-2048 only, no hybrid	Standard deployment but fully Shor-vulnerable. Most common finding.
8	ECDSA P-256 / ECDH P-256 only	Smaller key, same Shor vulnerability. Slightly less harvesting value due to ephemeral key exchange.

7	RSA-4096 only	Larger key delays classical attack but provides no quantum protection.
6	ECDH P-384 / ECDSA P-384	Slightly stronger curve, same quantum vulnerability.
5	Mixed RSA/ECC + AES-128	Symmetric component weakened by Grover's (64-bit effective). Asymmetric fully vulnerable.
4	RSA/ECC + AES-256	Symmetric component quantum-safe (128-bit effective). Asymmetric still vulnerable. Key exchange is the weak link.
2	Hybrid (X25519Kyber768 or equivalent)	PQC hybrid deployment. Classical algorithm provides backward compatibility; PQC algorithm provides quantum resistance. Residual risk from implementation flaws.
1	ML-KEM + ML-DSA deployed, classical deprecated	Near-complete PQC migration. Minor residual risk from algorithm maturity.
0	Fully quantum-safe (ML-KEM, ML-DSA, SLH-DSA, AES-256)	No known quantum vulnerability. Score cannot be 0 if any Shor-vulnerable algorithm remains in the certificate chain or key exchange.

Scoring Rules:

1. The score is determined by the **weakest** algorithm in the scanned configuration (weakest-link principle)
2. If multiple endpoints are scanned, the **highest** (worst) score across all endpoints is used
3. Certificate chain algorithms are scored separately from key exchange algorithms; the worse score applies
4. DKIM, SPF, and other email-infrastructure keys count if detected in DNS enumeration

3.3 Factor 3: Adversary Capability (Weight: 20%)

Definition: The sophistication, resources, and known harvesting infrastructure of threat actors likely to target the assessed organization.

Measurement: User-provided during assessment intake, supplemented by industry-specific threat intelligence defaults.

Score Scale (0-10):

Score	Threat Actor Profile	Indicators
10	Confirmed nation-state APT targeting	Organization appears in threat intel as a named target of state-sponsored groups (APT28, APT29, APT41, Lazarus Group, etc.). Active indicators of compromise or known harvesting campaigns.
8	Nation-state sector targeting	Organization operates in a sector known to be systematically targeted by nation-state actors (defense, energy, telecom, government) even without specific organizational targeting evidence.
6	Advanced persistent threat (non-state)	Sophisticated criminal enterprises or hacktivist groups with demonstrated cryptographic capability. Ransomware groups known to exfiltrate data before encryption.
4	Organized cybercrime	Financially motivated groups conducting broad campaigns. Data theft as secondary objective to ransomware. Limited storage infrastructure for long-term HNDL.
2	Opportunistic / Automated	Script kiddies, automated scanners, low-sophistication attackers. Unlikely to possess storage infrastructure for bulk encrypted traffic capture.
0	No external threat concern	Air-gapped systems with no network exposure, or data with zero adversary value. Extremely rare in practice.

Industry Defaults (QScout public-intake estimate):

Industry	Default Score	Justification
Federal / Defense	8	Systematic nation-state targeting documented
Financial Services	7	Documented APT targeting for SWIFT, trading systems
Healthcare	5	Ransomware targeting, but HNDL-specific harvesting less documented
Critical Infrastructure	7	Volt Typhoon, Sandworm, documented OT targeting
Technology	5	IP theft campaigns documented (APT10, APT41)
Retail	3	Financially motivated, less HNDL-relevant

General / Unknown	4	Conservative mid-range

3.4 Factor 4: Timeline Proximity (Weight: 15%)

Definition: How close the estimated CRQC arrival is relative to the present date, accounting for uncertainty.

Measurement: Computed from the Break Year Calculation (Section 4), which produces a confidence interval. Timeline Proximity uses the **left-tail** (earliest plausible) estimate.

Score Scale (0-10):

Score	Years Until Left-Tail CRQC	Scenario
10	0-2 years (CRQC imminent)	Aggressive: breakthrough announced or strongly indicated
9	2-3 years	Near-term: significant hardware milestones achieved
8	3-4 years	Short-term: error correction thresholds crossed
7	4-5 years	Matches readiness/control planning window
6	5-7 years	Planning horizon: NIST/CNSA 2.0 transition window
5	7-10 years	Moderate: consensus estimate range
4	10-12 years	Extended: slower-than-expected progress
3	12-15 years	Conservative: significant technical barriers remain
2	15-20 years	Distant: fundamental challenges unresolved
0	20+ years	Remote: no credible near-term CRQC pathway

Computation:

```
years_to_left_tail = Break_Year_Low - Current_Year
Timeline_Proximity_Score = max(0, min(10, 10 - (years_to_left_tail - 2) * (10/18)
```

This formula maps 2 years to score 10 and 20 years to score 0, with linear interpolation.

3.5 Factor 5: Active Targeting Profile (Weight: 10%)

Definition: Whether the specific organization (not just its sector) shows indicators of being actively targeted for data harvesting.

Measurement: Combination of scan-derived signals and industry context.

Score Scale (0-10):

Score	Targeting Indicators	Evidence Sources
10	Confirmed HNDL harvesting against this organization	Threat intel feeds, CISA alerts naming the organization, incident response findings
8	Organization in active APT campaign scope	Sector-specific CISA advisories, ally intelligence sharing, vendor threat reports
6	High-value target indicators present	Large attack surface, internet-facing APIs processing sensitive data, geopolitically sensitive operations
4	Moderate exposure	Standard enterprise internet footprint, some sensitive data processing
2	Low profile	Small attack surface, internal-only operations, minimal internet exposure
0	No targeting indicators	Air-gapped, no internet presence, no sensitive data

Intake-Derived Signals (QScout public intake):

- Subdomain count (proxy for attack surface): >50 subdomains = +2, >100 = +3
- Internet-facing services detected: Each additional service type = +1 (max +3)
- Geopolitical exposure: Domain registered in or serving sanctioned/adversarial regions = +2
- Industry sector adjustment: Applied per industry default table

Public Intake Default: Score 4 (moderate exposure) unless scan signals adjust upward.

3.6 Factor 6: Present Crypto Hygiene (Weight: 5%)

Definition: The quality of the organization's current classical cryptographic implementation, independent of quantum vulnerability.

Measurement: Directly derived from scan data.

Score Scale (0-10):

Score	Crypto Hygiene State	Indicators
10	Critically poor	TLS 1.0/1.1 enabled, SSL v3, MD5 in certificate chain, 3DES cipher suites, expired certificates
8	Poor	Weak cipher suites (RC4, DES), no HSTS, certificate approaching expiry, missing OCSP stapling
6	Below average	TLS 1.2 only with weak cipher preferences, SHA-1 in non-leaf certificates, no CT logs
4	Average	TLS 1.2 with good cipher suites, valid certificates, basic security headers
2	Good	TLS 1.3 preferred, strong cipher suites, comprehensive security headers, DNSSEC
0	Excellent	TLS 1.3 only, perfect forward secrecy, complete security headers, certificate transparency, DANE

Scoring Deductions (additive from baseline 0):

Finding	Deduction
TLS 1.0/1.1 supported	+4
SSL v3 supported	+5
3DES or RC4 cipher suites	+3
MD5 in any certificate	+4
SHA-1 in non-leaf certificate	+2
Missing HSTS	+1
Missing OCSP stapling	+1
No TLS 1.3 support	+1

Expired or soon-to-expire certificate (<30 days)	+2
Weak DH parameters (<2048-bit)	+2
No certificate transparency	+1
Missing Content-Security-Policy	+0.5

Final score = min(10, sum of deductions). A fully clean scan produces score 0.

3.7 Factor 7: Data Retention Window (Weight: 5%)

Definition: How long the organization's data must remain confidential, measured from today.

Measurement: User-provided during assessment intake, or derived from regulatory defaults.

Score Scale (0-10):

Score	Retention Requirement	Examples
10	Indefinite / 25+ years	Classified national security, state secrets, nuclear materials data
8	15-25 years	Long-term trade secrets, government records, infrastructure designs
7	10-15 years	Healthcare records (HIPAA: 6-10yr), financial records (SOX: 7yr + litigation holds)
5	5-10 years	Standard business contracts, employment records, tax filings
3	2-5 years	Marketing data, operational logs, short-term project data
1	6 months - 2 years	Session data, temporary credentials, short-lived tokens
0	Ephemeral / < 6 months	Real-time streaming data, no retention requirement

Regulatory Defaults:

Industry	Default Score	Assumed Retention	Regulatory Basis

Federal / Defense	8	15-25 years	NARA records schedules, classified retention
Healthcare	7	10-15 years	HIPAA: 6 years minimum; state laws often longer
Financial Services	7	10-15 years	SOX: 7 years; FINRA: 6 years; plus litigation holds
Legal	7	10-15 years	Attorney-client privilege, statute of limitations
Critical Infrastructure	6	5-10 years	NERC CIP record retention requirements
Technology	4	2-5 years	SOC 2 requirements, customer contracts
Retail	3	2-5 years	PCI DSS: 1 year minimum; state consumer protection laws
General / Unknown	5	5-10 years	Conservative mid-range

4. Break Year Calculation

4.1 Purpose

The "break year" is the estimated year by which a cryptographically-relevant quantum computer (CRQC) is expected to be capable of running Shor's algorithm at sufficient scale to break RSA-2048 or equivalent.

Critical Design Decision: QScout does NOT produce a single point-estimate break year. It produces a **confidence interval** with three named scenarios.

4.2 Input Sources

Source	Data Point	Citation
Global Risk Institute (GRI)	32-expert elicitation, probabilistic timeline	2024 Quantum Threat Timeline Report, December 2024
NIST IR 8547	Algorithm deprecation timeline, transition milestones	Transition to Post-Quantum Cryptography Standards, November 2024
NSA CNSA 2.0	Algorithm deprecation deadlines for NSS	CNSA 2.0 FAQ, September 2022
Published hardware milestones	Qubit counts, error rates, logical qubit demonstrations	IBM, Google, Quantinuum roadmaps (updated quarterly)

4.3 The Three Scenarios

QScout presents THREE named scenarios, not a single date:

Scenario	Break Year	Probability Basis	Source
Left-Tail (Aggressive)	**2029**	5-14% of GRI experts believe CRQC by this date	GRI 2024: "5-year horizon"

Planning (Moderate)	**2034**	19-34% of GRI experts believe CRQC by this date	GRI 2024: "10-year horizon"
Median (Conservative)	**2035**	50th percentile of expert estimates	GRI 2024: median forecast

4.4 Confidence Interval Specification

Every QScout report MUST present the break year as a range:

```
Quantum Break Window: 2029-2035
  Readiness/control planning target: 2029
  Planning basis (19-34% probability): 2034
  Median expert estimate: 2035
```

Rules for reports:

1. NEVER state a single break year without the full range
2. Always cite GRI 2024 as the primary source with the URL
3. Always specify that these are expert-elicitation probabilities, not predictions
4. Always note that the user should select a scenario based on their risk tolerance

4.5 Algorithm-Specific Break Year Adjustments

While the primary break year assumes Shor's algorithm targeting RSA-2048 / ECC P-256, specific algorithms may have adjusted timelines:

Algorithm	Adjustment	Rationale
RSA-1024	-2 years	Requires fewer logical qubits; potentially breakable earlier
RSA-2048	Baseline (no adjustment)	Primary target for break year estimates
RSA-4096	+1 year	Requires ~2x logical qubits; marginal additional time
ECC P-256	-1 year	Requires fewer qubits than RSA-2048 for Shor's
ECC P-384	Baseline	Similar qubit requirements to RSA-2048

AES-128	+5 years	Grover's provides only quadratic speedup; 2^64 still substantial
AES-256	+15 years	Grover's reduces to 2^128; effectively quantum-safe

4.6 Quarterly Update Process

Break year estimates are reviewed quarterly against:

1. Published GRI updates (annual)
2. Hardware milestone announcements (IBM, Google, Quantinuum roadmaps)
3. NIST transition guidance updates
4. Peer-reviewed advances in quantum error correction

Any revision to break year scenarios triggers a version increment of this methodology document.

5. Migration Deadline Calculation

5.1 Formula

The migration deadline is the date by which an organization should **begin** PQC migration to complete before the break year:

```
Migration_Start_Deadline = Break_Year_Scenario - Migration_Duration - Buffer_Year
```

5.2 Migration Duration Estimates

Migration duration depends on organizational complexity:

Complexity Level	Duration	Characteristics
Agile	2 years	Cloud-native architecture, crypto-agile design, <1000 cryptographic endpoints, strong DevOps
Typical	3 years	Standard enterprise, mixed cloud/on-prem, 1000-10,000 endpoints, some vendor dependencies

Complex	5 years	Large enterprise, legacy systems, 10,000+ endpoints, significant vendor/hardware dependencies
Regulated	8 years	Defense, critical infrastructure, or highly regulated environments with FIPS validation, hardware refresh cycles, and multi-agency coordination

Determination:

- **QScout public-intake package:** Estimated from technology stack fingerprinting. Default = Typical (3 years) unless indicators suggest otherwise.
- **QScout Silver or Gold:** User-provided based on detailed cryptographic inventory.

5.3 Buffer Years

Safety margin for delays, scope changes, and unforeseen complications:

Buffer	Use Case
0 years	Aggressive timeline, confident in execution capability
1 year	Standard buffer for well-managed programs
2 years	Conservative buffer accounting for vendor delays
3 years	Maximum buffer for regulated environments with certification requirements

Default: 1 year for QScout public-intake estimates.

5.4 Worked Examples

Example 1: Federal Government Agency (Planning Scenario)

```
Break_Year = 2034 (Planning scenario)
Migration_Duration = 8 years (Regulated complexity)
Buffer = 2 years

Migration_Start_Deadline = 2034 - 8 - 2 = 2024
```

```
Result: Organization should have begun migration in 2024.
Current year 2026: Organization is 2 YEARS BEHIND recommended start date.
```

Example 2: Cloud-Native SaaS Company (Planning Scenario)

```
Break_Year = 2034 (Planning scenario)
Migration_Duration = 2 years (Agile complexity)
Buffer = 1 year

Migration_Start_Deadline = 2034 - 2 - 1 = 2031

Result: Migration should begin by 2031. 5 years of preparation time.
```

Example 3: Healthcare System (Left-Tail Scenario)

```
Break_Year = 2029 (Left-tail / aggressive scenario)
Migration_Duration = 5 years (Complex)
Buffer = 1 year

Migration_Start_Deadline = 2029 - 5 - 1 = 2023

Result: Organization should have begun migration in 2023.
Current year 2026: Organization is 3 YEARS BEHIND recommended start date.
```

5.5 Migration Deadline in Reports

Reports MUST present the migration deadline as follows:

```
PQC Migration Deadline

Based on your assessment:
  Planning scenario (2034): Start migration by [DATE]
  Left-tail scenario (2029): Start migration by [DATE]

  Migration complexity: [LEVEL] (~[N] years)
  Buffer: [N] years
```

```
Status: [ON TRACK / X YEARS BEHIND]
```

Single-date Display: When space constrains display to a single date (e.g., dashboard widgets), use the **Planning scenario** deadline. Always include a footnote or tooltip explaining this is one of three scenarios.

6. QScout Assessment Methodology

6.1 QScout Public Intake: Consented Public-Surface Assessment

QScout public intake supports operator-reviewed, non-exploitative public checks:

Check	Method	Output
TLS Configuration	Handshake analysis	Protocol version, cipher suites, key exchange
Certificate Chain	X.509 inspection	Key algorithms, chain validity, CT logs
Key Exchange	ClientHello analysis	ECDH/RSA/hybrid/PQC detection
Security Headers	HTTP response analysis	HSTS, CSP, security policies
DNS Security	Record enumeration	DNSSEC, CAA, SPF/DKIM key analysis
Subdomain Discovery	Same-domain public discovery	Public target mapping
Email Infrastructure	DNS-based analysis	DKIM key sizes, MTA-STS, DANE

6.2 Factor Derivation from QScout public intake

Factor	Derivation Method
Data Sensitivity (25%)	Industry default (see Section 3.1)
Future Decrypt Risk (20%)	**Directly measured** from TLS cipher suites, certificate key types, key exchange algorithms

Adversary Capability (20%)	Industry default (see Section 3.3)
Timeline Proximity (15%)	**Computed** from break year calculation (Section 4)
Active Targeting Profile (10%)	**Partially measured** from subdomain count, service count; partially from industry default
Present Crypto Hygiene (5%)	**Directly measured** from TLS version, cipher suites, headers, certificates
Data Retention Window (5%)	Industry default (see Section 3.7)

6.3 Surface, Silver, and Gold: Governed Assessment Depth

Governed QScout paths replace defaults with approved measurements:

- **QScout Surface:** All approved public domains and exposed assets, no credentials = stronger external exposure and targeting evidence
- **QScout Silver:** Approved credentials and application, source, build, dependency, authenticated workflow, and integration evidence = stronger control and ownership evidence
- **QScout Gold:** Approved privileged infrastructure, runtime, telemetry, CBOM, cryptographic inventory, and governed evidence package = deepest measured baseline

7. Frontend Calculator Alignment

7.1 Purpose

The interactive HNDL Risk Calculator at `/risk-calculator` provides a self-service estimation tool. It MUST produce results directionally consistent with the backend scoring, though it accepts different (user-friendly) inputs.

7.2 Calculator Input Mapping

The frontend calculator collects 7 wizard-style inputs that map to the 7 backend factors:

Calculator Input	Backend Factor	Mapping
Industry	Data Sensitivity (25%) + Adversary Capability (20%) + Data Retention (5%)	Industry selection determines defaults for three factors simultaneously
Confidentiality Horizon	Data Retention Window (5%) + Timeline Proximity (15%)	Directly maps to retention; affects timeline urgency calculation
Data Types (multi-select)	Data Sensitivity (25%)	Refines sensitivity score based on specific data types (ePHI, PCI, trade secrets)
Exposure Surface	Active Targeting Profile (10%)	Internet-facing = higher targeting profile
Crypto Posture	Future Decrypt Risk (20%)	RSA/ECC only = high risk; piloting PQC = low risk
Crypto Locations	Present Crypto Hygiene (5%)	Breadth of cryptographic deployment affects hygiene assessment
Change Friction	(Migration deadline only)	Vendor vs. self-controlled affects migration duration estimate

7.3 Score Normalization

The frontend calculator normalizes to the same 0-100 scale using the same weight distribution. The calculator code MUST:

1. Apply the same weight percentages (25/20/20/15/10/5/5)
2. Use the same risk level thresholds (Critical >= 80, High >= 60, Medium >= 40, Low < 40)
3. Display the same break year confidence interval (not a point estimate)
4. Compute migration deadline using the same formula (Section 5)

7.4 Discrepancy Tolerance

Because the frontend uses simplified self-reported inputs while the backend uses scan data, scores may differ. Acceptable variance:

- **Within 15 points:** Normal variance from input precision differences
- **15-25 points:** Should be explained by specific factor differences (e.g., user reported "mixed crypto" but scan found RSA-only)
- **>25 points:** Indicates a methodology alignment defect that must be investigated

8. CNSA 2.0 Alignment

8.1 NSA CNSA 2.0 Timeline Requirements

QScout explicitly references and aligns with the NSA Commercial National Security Algorithm Suite 2.0 transition timeline:

Requirement	CNSA 2.0 Deadline	QScout Treatment
Software and firmware signing	**2025** (prefer CNSA 2.0 immediately)	Flag as OVERDUE if ML-DSA not deployed for code signing
Web servers/browsers, cloud services	**2025** (prefer) to **2033** (required)	Score based on hybrid TLS deployment status
Traditional networking equipment	**2026** to **2030**	Flag based on VPN/IPsec PQC status
Operating systems	**2025** to **2030**	Check for PQC-capable OS versions
Niche equipment (IoT, embedded)	**2030** to **2033**	Adjust migration complexity for hardware constraints

Custom/legacy applications	**2030** to **2033**	Factor into migration duration estimate

8.2 CNSA 2.0 Algorithm Requirements

QScout validates against CNSA 2.0 approved algorithms:

Use Case	CNSA 2.0 Required Algorithm	QScout Check
Key Establishment	ML-KEM-1024 (FIPS 203)	Check for ML-KEM in TLS key exchange
Digital Signatures	ML-DSA-87 (FIPS 204) or SLH-DSA (FIPS 205)	Check certificate signature algorithms
Symmetric Encryption	AES-256	Check cipher suite symmetric component
Hashing	SHA-384 or SHA-512	Check TLS and certificate hash algorithms

8.3 Report CNSA 2.0 Section

Every QScout report includes a CNSA 2.0 alignment section:

```
CNSA 2.0 Alignment Status: [NOT STARTED / IN PROGRESS / ALIGNED]

Findings:
  Key Exchange: [RSA-2048 detected — CNSA 2.0 alignment review flags ML-KEM-1024
  Signatures: [ECDSA P-256 detected — CNSA 2.0 alignment review flags ML-DSA-87 m
  Symmetric: [AES-256 detected — ALIGNED]
  Hashing: [SHA-256 detected — CNSA 2.0 prefers SHA-384+]
```

9. Validation Framework

9.1 What Constitutes Credible Validation

QScout methodology claims are subject to the following validation requirements:

Claim Type	Required Evidence	Current Status
Methodology soundness	Independent expert review	Annual review by external cybersecurity experts; review letters available under NDA
Statistical accuracy	Backtesting against known outcomes	N/A for quantum timeline predictions (no ground truth yet exists)
Scan accuracy	False positive/negative rates	<5% false positive rate per customer re-validation on representative enterprise reassessment samples
Score reproducibility	Same inputs produce same outputs	Deterministic algorithm; reproducible by design

9.2 What We Do NOT Claim

1. **We do not claim "expert panel validation" without naming the panel.** Any reference to expert validation must specify: reviewer identity or institutional affiliation, scope of review, date of review, and whether the review letter is available.
2. **We do not predict when CRQC will arrive.** We present expert-elicitation probability distributions from published research (GRI) and let users select planning scenarios.
3. **We do not claim our scores are statistically validated against breach outcomes.** HNDL has not yet been exploited at scale; there is no ground truth to validate against. Our scores are risk indicators based on factor analysis, not actuarial predictions.

9.3 Annual Methodology Review

Each annual review covers:

1. **Factor definitions:** Are the 7 factors still the right decomposition of HNDL risk?
2. **Weight calibration:** Do the weights still reflect the relative importance of factors?
3. **Break year inputs:** Have GRI, NIST, or hardware milestones materially changed?
4. **Score distribution:** Are scores clustering in a useful range, or do weights need adjustment?
5. **False positive analysis:** What percentage of findings were confirmed vs. disputed by customers?

Review findings are documented in a versioned review letter available under NDA.

9.4 Path to Formal Validation

For organizations requiring stronger validation claims, Qtonic Quantum offers:

1. **Methodology briefing:** 60-minute technical walk-through with customer's security team
2. **NDA-protected review letter:** Signed letter from external reviewer documenting scope, findings, and limitations
3. **Reproducibility package:** Complete input/output documentation for a customer's scan, enabling independent score verification
4. **Open methodology:** This document itself serves as the reproducibility specification -- any party can verify score computation given the same inputs

10. Interpreting Your HNDL Score

10.1 Score Context

An HNDL score is **not** a traditional vulnerability score. It represents:

> *The scenario-weighted exposure to future decryption of currently-harvested data, expressed as a composite risk index on a 0-100 scale.*

A score of 70 does NOT mean "70% chance of breach." It means:

- Your cryptographic posture has significant quantum vulnerability
- Your data sensitivity and retention extend into the CRQC timeline
- Adversary capability and targeting profile indicate harvesting is plausible
- Migration should be prioritized within 6 months

10.2 Recommended Actions by Score

Score	Priority	Timeline	Actions
80-100	P0 (Immediate)	30 days	Emergency cryptographic inventory, PQC hybrid deployment on high-value endpoints, board-level risk briefing
60-79	P1 (Quarter)	90 days	Complete cryptographic inventory, begin PQC migration planning, vendor PQC roadmap assessment
40-59	P2 (Semi-annual)	6 months	Include PQC in security roadmap, pilot hybrid TLS on non-critical endpoints, establish crypto-agility requirements
20-39	P3 (Annual)	12 months	Annual reassessment, ensure crypto-agility in new procurements, monitor quantum developments
0-19	Maintain	Ongoing	Continue current practices, maintain PQC awareness, reassess if score inputs change

10.3 Comparison Benchmarks

Based on QScout scan data (as of February 2026):

Percentile	Score	Interpretation
Top 10%	< 25	PQC adoption leaders (hybrid TLS deployed)
Top 25%	25-40	Proactive posture (PQC pilots underway)
Median	45-55	Average enterprise (RSA/ECC only, planning stage)
Bottom 25%	60-75	Elevated risk (no PQC activity, sensitive data)
Bottom 10%	> 75	Critical exposure (legacy crypto + high-value data)

11. Limitations and Disclaimers

11.1 Scope Limitations

- QScout public-intake packageting is **external, consented, and non-exploitative public-surface checking only**
- Internal cryptographic usage cannot be detected without authenticated access
- Third-party/vendor cryptographic posture is not assessed at public-intake scope
- Mobile applications and IoT devices require QScout Silver or Gold evaluation
- Content delivery networks (CDNs) and reverse proxies may mask origin server cryptography

11.2 Assumptions

- CRQC timeline estimates are based on published expert elicitation, not prediction
- Adversary capability to harvest traffic is assumed for internet-facing systems
- Algorithm vulnerability ratings assume correct implementation of Shor's/Grover's algorithms
- Migration duration estimates assume reasonable organizational commitment and budget

11.3 Not a Guarantee

QScout HNDL scores are **risk indicators**, not guarantees. They:

- Do not predict specific breach events

- Do not constitute compliance certification
- Do not replace comprehensive security assessments
- Should be combined with organizational context that only the customer possesses

11.4 Known Limitations of the Model

1. **No ground truth:** HNDL exploitation has not occurred at scale; all scoring is prospective
2. **Expert disagreement:** GRI experts range from 5% to 34% probability by 2034; the field is genuinely uncertain
3. **Classified programs:** Some quantum computing progress may be classified; public estimates may understate capability
4. **Post-quantum algorithm maturity:** ML-KEM, ML-DSA, and SLH-DSA are newly standardized; implementation vulnerabilities may emerge
5. **Symmetric algorithm assumptions:** Grover's algorithm quadratic speedup is well-established but may not be practically achievable at scale

12. References

12.1 Primary Sources

1. **GRI (2024).** *Quantum Threat Timeline Report.* Global Risk Institute, December 2024. 32-expert elicitation. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
2. **NIST (2024).** *IR 8547: Transition to Post-Quantum Cryptography Standards.* Initial Public Draft, November 2024. https://csrc.nist.gov/pubs/ir/8547/ipd
3. **NSA (2022).** *CNSA 2.0 Cybersecurity Advisory: Commercial National Security Algorithm Suite.* September 2022. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
4. **NIST (2024).** *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM).* August 2024. https://csrc.nist.gov/pubs/fips/203/final
5. **NIST (2024).** *FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA).* August 2024. https://csrc.nist.gov/pubs/fips/204/final
6. **NIST (2024).** *FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA).* August 2024. https://csrc.nist.gov/pubs/fips/205/final

12.2 Supporting Sources

7. **CISA (2024).** *Post-Quantum Cryptography Initiative.* https://www.cisa.gov/quantum
8. **White House (2021).** *Executive Order 14028: Improving the Nation's Cybersecurity.* May 12, 2021.
9. **OMB (2022).** *M-23-02: Migrating to Post-Quantum Cryptography.* November 18, 2022.
10. **IBM/Ponemon (2024).** *Cost of a Data Breach Report 2024.* $4.88M global average. https://www.ibm.com/reports/data-breach
11. **Federal Reserve (2025).** *Quantum Computing: Implications for Financial Services.* FEDS Notes, 2025. https://doi.org/10.17016/FEDS.2025.093
12. **G7 Cyber Expert Group (2022).** *Post-Quantum Cryptography Roadmap.* https://www.g7germany.de/resource/blob/974430/2153140/data.pdf

12.3 Hardware Milestone References

13. **IBM (2025).** *Quantum Development Roadmap.* https://www.ibm.com/quantum/roadmap
14. **Google (2024).** *Willow: Quantum error correction below threshold.* Nature, December 2024.
15. **Quantinuum (2025).** *H-Series Quantum Computing Roadmap.*

13. Appendix A: Complete Scoring Worked Example

Scenario: Mid-size healthcare system, QScout public-intake package

Scan Findings:

- TLS 1.2 only (no TLS 1.3)
- RSA-2048 certificate, ECDHE key exchange
- Missing HSTS on some subdomains
- DKIM with RSA-1024
- 35 subdomains discovered
- No PQC/hybrid TLS detected

Factor Scoring:

Factor	Weight	Raw Score	Normalized	Weighted
Data Sensitivity	25%	6 (PHI/Healthcare default)	60	15.0
Future Decrypt Risk	20%	9 (RSA-2048 only, ECDHE = Shor-vulnerable)	90	18.0
Adversary Capability	20%	5 (Healthcare default)	50	10.0
Timeline Proximity	15%	7 (Left-tail 2029 = 3 years out)	70	10.5
Active Targeting Profile	10%	4 (Moderate: 35 subdomains, healthcare sector)	40	4.0
Present Crypto Hygiene	5%	4 (TLS 1.2 only +1, missing HSTS +1, DKIM RSA-1024 +2)	40	2.0
Data Retention Window	5%	7 (Healthcare: 10-15yr default)	70	3.5

Composite Score: 15.0 + 18.0 + 10.0 + 10.5 + 4.0 + 2.0 + 3.5 = **63.0**

Risk Level: HIGH (>= 60)

Break Year:

```
Readiness/control date: 2029
Planning: 2034 (19-34% probability)
Median: 2035
```

Migration Deadline (Planning Scenario):

```
2034 - 5 (Complex) - 1 (Buffer) = 2028
Status: 2 years remaining before recommended start
```

14. Appendix B: Changelog from v1.0

Item	v1.0	v2.0	Reason
Factor count	6	7	Added Active Targeting Profile; separated Adversary Capability from targeting indicators
Factor names	Cryptographic Vulnerability, Data Longevity, Exposure Surface, Migration Complexity	Future Decrypt Risk, Data Retention Window, Active Targeting Profile, Present Crypto Hygiene	Names now reflect what is measured, not how it is measured
Weights	25/25/20/15/10/5	25/20/20/15/10/5/5	Adversary Capability elevated to 20% from 5%; Data Sensitivity remains 25%; new factors at 5%
Break year	Single date (2030 or 2032 or 2034 depending on context)	Confidence interval with 3 named scenarios (2029/2034/2035)	Eliminated contradictory point estimates
Migration deadline	Inconsistent (2027-01-01 vs 2027-08-09 appeared in different contexts)	Single deterministic formula: Break_Year - Migration_Duration - Buffer	Formula published, reproducible

Timeline Multiplier	0.8 / 1.0 / 1.3 multiplier applied post-scoring	Eliminated; timeline incorporated as Factor 4 (Timeline Proximity)	Multiplicative adjustments caused score instability
Expert validation	Unsourced "validated by expert panel" claim removed	Validation framework with specific requirements (Section 9)	No unsourced claims
CNSA 2.0	Referenced but not mapped	Explicit algorithm-by-deadline mapping (Section 8)	Actionable compliance alignment

15. Contact

For questions about QScout methodology, to request a methodology briefing, or to schedule an enterprise assessment:

Qtonic Quantum Corp
Email: info@qtonicquantum.com
Phone: +1 (866) 4-QTONIC
Web: https://qtonicquantum.com
Methodology: https://qtonicquantum.com/methodology

Version 2.0 | February 2026
This document is the authoritative specification for QScout HNDL risk scoring.
Any implementation that deviates from this specification is a defect.

Post-Quantum Ready, Continuously.