STØRMRUNE

A HIVESTØRM MODULE · THE DISCOVERY LAYER

POST-QUANTUM CRYPTOGRAPHIC READINESS

# Cryptographic Posture Assessment

## *Prepared for Meridian Financial Group*

SAMPLE REPORT · ILLUSTRATIVE DATA · NOT A REAL CLIENT

| | |
|---|---|
| ASSESSMENT REF | SR-2026-0417-MFG |
| ASSESSMENT DATE | 17 April 2026 |
| SCOPE | Trading & settlement estate · 4 network segments |
| METHOD | Passive discovery + active discovery (Tier 1–2) |
| ENGINE | StørmRune Assessment Engine v0.9 |
| CLASSIFICATION | Commercial in Confidence |

# Executive Summary

01

StørmRune discovered **847 cryptographic operations** across **124 endpoints** in the trading and settlement estate. Each was graded from A+ to F for quantum readiness and weighted for harvest-now-decrypt-later exposure. This report produces the evidence that supports Meridian Financial Group's post-quantum migration planning against the CNSA 2.0 timeline.

| 847 | 12% | 26% | 296 |
|---|---|---|---|
| CRYPTOGRAPHIC OPERATIONS DISCOVERED | CNSA 2.0 COMPLIANT (A+) | REQUIRE IMMEDIATE ACTION (D & F) | ENDPOINTS ON QUANTUM-WEAK CRYPTO |

◆ HEADLINE FINDING

The settlement estate carries **ten-year-sensitivity transaction data** across 296 endpoints negotiating RSA-2048 and ECDHE-P-256 (Grade C). This is the estate's highest harvest-now-decrypt-later exposure: data intercepted today remains recoverable once a cryptographically-relevant quantum computer exists — well within the sensitivity lifetime of settlement records.

## Top Priority Findings

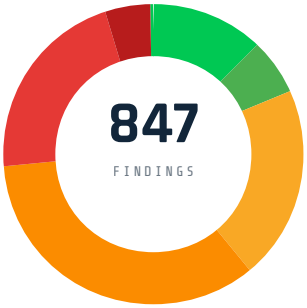
| GRADE | FINDING | EXPOSURE |
|---|---|---|
| F | **3 production certificates expired; 12 self-signed on external-facing services** | Trust integrity failure · exploitable today, quantum aside |
| D | **Settlement gateway cluster negotiating 3DES and SHA-1 certificate signatures** | Deprecated cryptography in a critical transaction path |
| C | **296 endpoints on RSA-2048 / ECDHE-P-256 carrying long-lived settlement data** | Highest HNDL exposure across the estate |

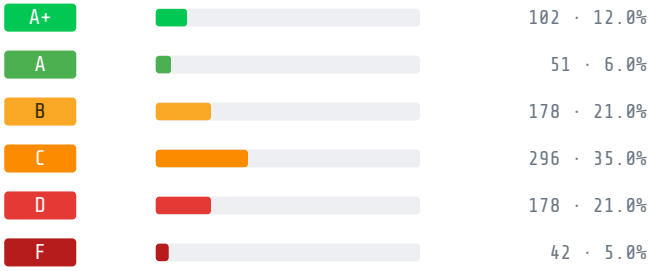
StørmRune discovers what needs protecting; *StørmTrust fills the gaps it finds.* A prioritised migration roadmap mapped to remediation is provided in Section 05.

# Grade Distribution

02

Every discovered cryptographic operation is assigned a single QuantumGrade from A+ (CNSA 2.0 compliant) to F (critical). The scale is weighted for harvest-now-decrypt-later risk and mapped to CNSA 2.0.



A+ A B C D F

| GRADE | POSTURE | WHAT IT MEANS |
|---|---|---|
| A+ | **CNSA 2.0 compliant** | ML-KEM, ML-DSA, AES-256, SHA-384+ · no quantum exposure |
| A | **PQC, not aligned** | Post-quantum deployed but not yet CNSA-aligned parameters |
| B | **Strong classical** | RSA-3072+, ECDHE-P-384+, AES-256 · quantum-vulnerable, no PQC |
| C | **Minimum classical** | RSA-2048, P-256, AES-128 · quantum-vulnerable · HNDL risk applies |
| D | **Deprecated / weak** | 3DES, SHA-1, RSA-1024, RC4 · exploitable today, quantum aside |
| F | **Critical** | No encryption, expired or self-signed certificates in production |

# Findings Detail



Representative findings ordered worst-grade first. Each carries its recommended migration target. The complete inventory of 847 findings is delivered as a machine-readable Cryptographic Bill of Materials (CBOM) alongside this report.

| GRADE | ENDPOINT | PROTOCOL | ALGORITHM | HNDL | MIGRATION TARGET |
|---|---|---|---|---|---|
| F | 10.4.2.19:443 | TLS 1.2 | Expired certificate (payments) | 1.00 | Reissue · ML-DSA-65 |
| F | 10.4.7.8:8443 | TLS 1.2 | Self-signed · external-facing | 1.00 | CA-issued · ML-DSA-65 |
| F | 10.2.1.44:80 | HTTP | No encryption (admin panel) | 1.00 | TLS 1.3 · AES-256-GCM |
| D | 10.4.3.10:443 | TLS 1.2 | 3DES-EDE-CBC-SHA | 1.00 | AES-256-GCM |
| D | 10.4.3.11:443 | TLS 1.2 | SHA-1 certificate signature | 1.00 | SHA-384 · ML-DSA-65 |
| D | 10.5.9.22:22 | SSH | ssh-rsa (1024) · dh-group1 | 1.00 | ssh-ed25519 · ML-KEM |
| D | 10.5.9.40:22 | SSH | hmac-sha1 · aes128-cbc | 1.00 | hmac-sha2-256 · aes256-gcm |
| C | 10.4.1.50:443 | TLS 1.2 | ECDHE-RSA · P-256 · AES-128 | 0.30 | ML-KEM-768 · AES-256-GCM |
| C | 10.4.1.51:443 | TLS 1.2 | RSA-2048 key exchange | 0.30 | ML-KEM-768 |
| C | 10.4.6.12:5432 | TLS 1.2 | RSA-2048 · AES-128-GCM | 0.30 | ML-DSA-44 · AES-256-GCM |
| B | 10.4.1.70:8443 | TLS 1.3 | X25519 · AES-256-GCM | 0.10 | ML-KEM-768 (hybrid) |
| B | 10.4.2.90:443 | TLS 1.2 | ECDHE-P-384 · AES-256-GCM | 0.10 | ML-KEM-1024 |
| A+ | 10.4.1.80:443 | TLS 1.3 | ML-KEM-768 · AES-256-GCM | 0.00 | — compliant |
| A+ | 10.4.8.5:443 | TLS 1.3 | ML-KEM-1024 · AES-256-GCM | 0.00 | — compliant |

HNDL = harvest-now-decrypt-later exposure score (0.00–1.00). Full inventory available as CBOM (JSON / CSV).

# Certificate Inventory

04

StørmRune discovered **218 X.509 certificates** across the estate. **34** expire within 90 days, **12** are self-signed on production external-facing services, and **3** are already expired and in active use.

| 218 | 34 | 12 | 3 |
|---|---|---|---|
| CERTIFICATES DISCOVERED | EXPIRING WITHIN 90 DAYS | SELF-SIGNED IN PRODUCTION | EXPIRED & IN ACTIVE USE |

| SUBJECT | KEY | SIG ALGORITHM | EXPIRY | STATUS | GRADE |
|---|---|---|---|---|---|
| pay-gw.meridian.internal | RSA-2048 | sha256WithRSA | 2026-03-02 | EXPIRED | F |
| *.dmz.meridian.io | RSA-2048 | sha256WithRSA | 2027-01-14 | SELF-SIGNED | F |
| legacy-settle.meridian.internal | RSA-2048 | sha1WithRSA | 2026-08-19 | SHA-1 | D |
| api.meridian.io | RSA-2048 | sha256WithRSA | 2026-06-30 | <90 DAYS | C |
| *.internal.meridian.io | RSA-2048 | sha256WithRSA | 2026-07-11 | <90 DAYS | C |
| trade-fix.meridian.internal | ECDSA P-384 | ecdsa-sha384 | 2027-05-20 | VALID | B |
| edge.meridian.io | ML-DSA-65 | ml-dsa-65 | 2027-09-01 | VALID | A+ |

◆ CERTIFICATE ESTATE NOTE

The predominance of **RSA-2048 with SHA-256** signatures across the certificate estate is the single largest migration workload. Under CNSA 2.0 these require transition to ML-DSA signing. The expired and self-signed certificates on external-facing services are a present-day trust-integrity issue independent of quantum exposure and warrant immediate remediation.

# Harvest-Now-Decrypt-Later Analysis

05

Harvest-now-decrypt-later (HNDL) exposure measures the risk that data intercepted today can be decrypted once a cryptographically-relevant quantum computer exists. StørmRune weights each finding by the data-sensitivity lifetime of the traffic it protects against the estimated quantum horizon.

| DATA CLASS | SENSITIVITY LIFE | ENDPOINTS | DOMINANT GRADE | HNDL EXPOSURE |
|---|---|---|---|---|
| **Settlement & transaction records** | 10 years | 296 | C | **HIGH** |
| **Client identity & KYC** | 7 years | 88 | C | **HIGH** |
| **Trading strategy / order flow** | 5 years | 64 | B | **MEDIUM** |
| **Operational telemetry** | 2 years | 120 | B | LOW |
| **Public market data** | <1 year | 31 | A+ | MINIMAL |

◆ PRIORITY EXPOSURE

**Settlement and transaction records** combine the longest sensitivity lifetime (ten years) with quantum-vulnerable Grade C cryptography across 296 endpoints. Data harvested from these flows today would remain recoverable throughout its entire confidentiality window. This is the estate's highest-priority migration target and the recommended first phase of remediation.

Sensitivity lifetimes shown are illustrative defaults for a financial-markets estate. StørmRune Enterprise permits per-data-class sensitivity and quantum-horizon configuration, refining the HNDL weighting to an organisation's own risk model.

# Migration Roadmap

06

Findings are grouped into a prioritised remediation plan. Each phase maps directly to *StørmTrust* — the post-quantum remediation module that consumes StørmRune's findings to configure crypto-agility across the estate.

## Phase 1 — Critical

0–30 DAYS · GRADE F & D

- → Reissue 3 expired production certificates; replace 12 self-signed external-facing certificates with CA-issued ML-DSA-65
- → Eliminate 3DES and SHA-1 from the settlement gateway cluster — transition to AES-256-GCM and SHA-384
- → Retire ssh-rsa (1024) and dh-group1 on management endpoints — deploy ssh-ed25519 with ML-KEM key exchange
- → Terminate the plaintext admin panel; enforce TLS 1.3

## Phase 2 — High (HNDL priority)

30–90 DAYS · GRADE C

- → Migrate 296 settlement endpoints from RSA-2048 / P-256 to ML-KEM-768 hybrid key exchange
- → Transition the RSA-2048 certificate estate to ML-DSA signing under a phased re-issuance programme
- → Upgrade AES-128 to AES-256-GCM across client-identity and KYC systems

## Phase 3 — Strengthen

90–180 DAYS · GRADE B

- → Move X25519 and ECDHE-P-384 endpoints to ML-KEM hybrid, aligning to CNSA 2.0 parameters
- → Establish continuous monitoring so posture does not silently regress after remediation
- → Extend post-quantum signing across the trading and settlement rail

◆ CONTINUOUS ASSURANCE

Cryptographic posture drifts as systems change. StørmRune Enterprise runs continuous discovery and alerts on new Grade D/F findings, algorithm downgrades and approaching certificate expiry — producing the ongoing evidence that supports a sustained CNSA 2.0 migration programme.

# Methodology & Notes

07

## How StørmRune discovers

StørmRune is a passive-first cryptographic discovery engine. In passive mode it reads a mirror of network traffic via a SPAN port and never transmits — it is approved for classified, operational-technology and air-gapped estates. Active discovery initiates benign TLS and SSH handshakes to internal targets to surface posture not observed passively; it uses no credentials and performs no exploitation. All processing and output remain local to the appliance or tenancy; nothing is transmitted to Hive Storm.

## How findings are graded

Each discovered algorithm is matched against StørmRune's cryptographic algorithm database and assigned a QuantumGrade from A+ to F, mapped to CNSA 2.0 and NIST FIPS 203–205. A connection is graded on its weakest component. Certificates are additionally assessed for expiry, self-signing and signature-algorithm strength. HNDL exposure is derived from data-sensitivity lifetime against the estimated quantum horizon.

## On compliance

This report **produces the evidence that supports** an organisation's post-quantum readiness and CNSA 2.0 migration planning. It does not certify, guarantee or satisfy any regulatory requirement, and it is not a substitute for formal audit. Certifications referenced by the Størm platform (including SOC 2, ISO 27001, ISO 42001 and FIPS 140-3) are on Hive Storm's certification roadmap.

> ◆ ABOUT THIS DOCUMENT
>
> This is a **sample report containing illustrative data** for a fictional organisation, produced to demonstrate the StørmRune assessment output. Endpoints, findings, certificates and figures shown are synthetic and do not represent any real client, network or benchmark. A live assessment reflects the actual cryptographic posture of the estate under review.

STØRMRUNE

Rune finds the gaps · StørmTrust fills them

Hive Storm Technologies · Apeirogon Holdings Corp
hivestorm.io · sales@hivestorm.io