Sample document. Every organisation named below is invented and every figure is illustrative. It is published so you can judge the output before booking a call. Use your browser's print to PDF to keep a copy; the watermark is part of the document.

See a single finding in detail

PENTHROPIC SECURITY · THIRD-PARTY ASSURANCE

Monthly vendor verification report

Prepared for: Meridian Group Ltd · Period: 1 to 30 June 2026 · Issued: 3 July 2026

1. Summary

Meridian's supplier register held 34 active vendors this period. All 34 were re-checked against public exposure and against the attestations held on file. Six findings were raised, of which two are high severity. Four findings from previous periods were closed.

34
Vendors verified

6
Findings raised

4
Findings closed

2. What was checked

Each vendor was assessed against two independent sources, then compared.

Attested. The questionnaire responses, certificates and reports held on file for that vendor.

Observed. Public certificate transparency, DNS and mail policy, published security headers, disclosed breach corpora, and the vendor's own published policy pages.

No active scanning was performed. No credentials were used. Every observation is reproducible from public sources.

3. Findings this period

Ordered by severity, then by date first seen.

REF	VENDOR	FINDING	SEVERITY	CONTROL
F–241	Northwind Analytics	SOC 2 attestation 19 months out of date while contract active	High	A.5.22
F–242	Calder Logistics	DMARC policy relaxed from reject to none during the period	High	A.5.23
F–243	Brightlane HR	New subdomain issued a certificate outside the declared estate	Medium	A.5.21
F–244	Orrell Print	Named data-protection contact has left; no replacement supplied	Medium	A.5.20
F–245	Vale Software	Sub-processor added without the contractual notice period	Medium	A.5.19
F–246	Tarn Media	Published privacy policy no longer names a UK representative	Low	A.5.34

4. Finding detail: F-242

Calder Logistics, DMARC policy relaxed during the period.

Attested	Questionnaire of 8 January 2026, question 6.1: email authentication is "enforced with DMARC at reject".
Observed	On 2 June the published DMARC record read `p=reject`. On 17 June it read `p=none`. It has remained at `p=none` since.
Delta	The control was in place at the time of assessment and was removed 5 months later. An annual questionnaire would have recorded this as compliant for a further 7 months.
Impact	Mail spoofing Calder's domain is no longer rejected by recipients. Calder issue delivery notifications to Meridian's customers, so the practical risk is phishing that appears to come from a trusted logistics partner.
Action	Raised with Calder on 18 June. Awaiting a date for restoring enforcement. Recommend a contractual notice requirement for material changes to email authentication.

This is the finding type that only continuous checking produces. Nothing was wrong at onboarding, and nothing was wrong at the last review.

5. Closed since last period

REF	VENDOR	RESOLUTION	DAYS OPEN
F–228	Halden Cloud	Current ISO 27001 certificate supplied, scope confirmed	21
F–231	Kelso Payments	Expired TLS certificate replaced	3
F–233	Ryehill Consulting	Risk accepted by the CISO, review date 1 December 2026	44

REF	VENDOR	RESOLUTION	DAYS OPEN
F–236	Brightlane HR	Sub-processor list updated and re-issued	12

6. Coverage statement

Stated honestly, including what this report does not cover.

Vendors in register	34
Vendors verified	34 (100%)
With an attestation on file	27 (79%)
Attestation current	22 (65%)
Not covered	Anything not observable from public sources or from documents you have given us. We do not test vendor systems and we do not assert what happens inside them.

7. Method and limitations

Observations are drawn from passive, publicly available sources only: certificate transparency logs, public DNS, published HTTP response headers, published policy pages, and public breach corpora. No system belonging to a vendor was scanned, probed or accessed.

A clean result means no gap was visible from those sources during the period. It is not a statement that a vendor is secure, and this report does not make one.

Penthropic Security Ltd · Sample document, not a client deliverable · Every organisation named is fictitious.