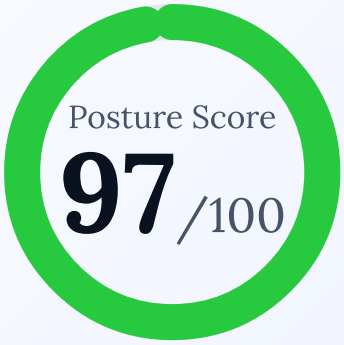
# MOORLI VendorRiskDiagnostic

**Audit ID:** cf73798d-90c3-4e9b-b3b4-bb1a3d5a4840 **Generated:** May 9, 2026, 12:02 AM UTC

**Plan:** EXECUTIVE **Vendors:** 1 **Client Company:** SAMPLE REPORT




Higher scores indicate stronger vendor email security across your supply chain.

A high overall score does not mean zero control failures. Review FAIL findings independently from the overall posture band.

## SECURITY POSTURE BY CATEGORY

| | | |
|---|---|---|
| **Spoofing** DMARC | | 94 |
| **Identity** SPF | | 94 |
| **Transport Maturity** MTA-STS / TLS-RPT adoption | | 50 |
| **Infra** MX / BIMI / DNSSEC | | 92 |

**Additional scoring signals:** This run includes 7 DKIM selector-rule observations and 4 external reputation-rule observations. DKIM selector checks and selected external reputation corroboration are included in vendor-level findings and overall risk scoring, but are not shown as standalone posture bars because DKIM selector discovery is best-effort and reputation signals are corroborative.

## RISK DISTRIBUTION

1 vendor domain

| CRITICAL | HIGH | MEDIUM | LOW |
|---|---|---|---|
| 0 domains | 0 domains | 0 domains | 1 domain |

All vendors pass baseline controls. 3 hardening opportunities were identified. The main hardening themes are DMARC policy is p=quarantine (good, but p=reject is stronger) and SPF ends in ~all (soft fail). Some receivers may still accept spoofed mail instead of rejecting it.

### Key Findings

⚠ moorli.io - SPF uses ~all (soft fail). Spoofed emails may still be accepted by some receivers instead of being rejected.

ℹ 1 of 1 vendor do not publish MTA-STS. This is a transport maturity gap, not a core control failure - industry adoption remains low. Prioritize MTA-STS for vendors handling invoices or payment instructions.

⚠ 1 of 1 vendor without DNSSEC. DNS records (including email routing) are more susceptible to tampering.

### Next 7 Days

1. **Share hardening recommendations with vendor contacts**
   `moorli.io`
2. **Schedule validation rescan to confirm remediation (recommended: 30 days)**

### Why This Matters

All vendors meet baseline security posture. The 3 warnings identified are hardening opportunities - addressing them would further reduce spoofing and interception risk across your vendor ecosystem.

*For clickable rule references, interactive filtering, and the show/hide PASS toggle, view the HTML version of this report.*

## Methodology

This assessment is performed using public DNS queries, lightweight public-web validation (for example, fetching an MTA-STS policy file when present), authoritative registration context lookups, and selected third-party reputation and threat-intelligence signals used as corroborating inputs. It does not require vendor access, authentication, or intrusive testing. Findings labeled **INFO** indicate optional or advisory controls that were not adopted or not fully configured. Findings labeled **NA** indicate that a prerequisite or source was unavailable and the check could not be deterministically evaluated. In some customer-facing

summaries, advisory-only NA findings may be displayed as INFO when the underlying condition reflects absence of an optional control rather than a source outage.

**Note on DKIM:** DKIM selectors are not predictable externally and cannot be exhaustively validated without internal configuration knowledge. Absence of a selector in this audit does not prove DKIM is not used.

# Vendor Risk Map

CRITICAL: 0 HIGH: 0 MEDIUM: 0 LOW: 1

### How Scores Work

**Risk Score** Per-vendor exposure rating (0–100). Higher means more risk. Derived from weighted FAIL/WARN findings across spoofing, identity, transport, and infrastructure controls. We weight **DMARC enforcement** heavily because it is the primary control that blocks unauthorized impersonation at the receiver.

CRITICAL ≥ 80 HIGH 60–79 MEDIUM 40–59 LOW < 40

| DOMAIN | RISK | RISK SCORE | TOP ISSUES |
|---|---|---|---|
| moorli.io | LOW | 3 | DMARC policy is p=quarantine (good, but p=reject is stronger). • SPF ends in ~all (soft fail). Some receivers may still accept spoofed mail instead of rejecting it. • DNSSEC is absent. Treat this as secondary hardening context, not a peer to DMARC/SPF enforcement failures. |

# Detailed Findings (per Domain)

Each domain begins on a new page for easy review.

## moorli.io `moorli.io`

**Findings** FAIL 0 · WARN 3 · PASS 23 · NA 16

Risk: LOW · Score: **3**

### Top Issues

DMARC policy is p=quarantine (good, but p=reject is stronger). • SPF ends in ~all (soft fail). Some receivers may still accept spoofed mail instead of rejecting it. • DNSSEC is absent. Treat this as secondary hardening context, not a peer to DMARC/SPF enforcement failures.

| STATUS | RULE | DETAILS | RECOMMENDATION |
|---|---|---|---|
| WARN | **VRD-DMARC-005** DMARC Enforcement (Spoofing Exposure) | DMARC policy is p=quarantine (good, but p=reject is stronger). | Encourage the vendor to move from p=quarantine to p=reject after they have confirmed legitimate mail is aligned. |
| WARN | **VRD-INFRA-024** Mail Infrastructure Hygiene | DNSSEC is absent. Treat this as secondary hardening context, not a peer to DMARC/SPF enforcement failures. | Ask vendor to enable DNSSEC where feasible. |
| WARN | **VRD-SPF-012** SPF Identity Controls (Sender Integrity) | SPF ends in ~all (soft fail). Some receivers may still accept spoofed mail instead of rejecting it. | Ask the vendor to converge on a single valid SPF record that ends in -all once they have confirmed all authorized senders are covered. |
| INFO | **VRD-ADV-019** Transport Security & Reporting (Maturity) | TLS-RPT is not published. Treat this as a maturity gap, not a discrete warning. | Ask vendor to publish TLS-RPT (_smtp._tls) to receive TLS failure reports. |
| INFO | **VRD-ADV-020** Transport Security & Reporting (Maturity) | MTA-STS is not adopted. Treat this as transport-maturity context, not a discrete warning. | Ask vendor to publish a valid MTA-STS TXT record and host a valid policy in testing or enforce mode. |

| STATUS | RULE | DETAILS | RECOMMENDATION |
|---|---|---|---|
| INFO | **VRD-ADV-021**<br>Transport Security & Reporting (Maturity) | No MTA-STS record; policy validation not applicable. | Ask vendor to host a valid policy at https://mta-sts./.well-known/mta-sts.txt and ensure it parses. |
| INFO | **VRD-ADV-033**<br>Transport Security & Reporting (Maturity) | No MTA-STS record; policy mode cannot be evaluated. | Ask vendor to move MTA-STS policy from 'testing' to 'enforce' once they have verified compatibility. |
| INFO | **VRD-DKIM-026**<br>DKIM Signing (Message Integrity) | No common selector responded, but selector guessing alone is not enough to conclude DKIM is absent. | Treat this as inconclusive unless message headers, vendor guidance, or known selectors confirm whether DKIM signing is enabled. |
| INFO | **VRD-DKIM-028**<br>DKIM Signing (Message Integrity) | No DKIM record found among probed selectors; syntax check not applicable. | Treat this as inconclusive unless message headers, vendor guidance, or known selectors confirm whether DKIM signing is enabled. |
| INFO | **VRD-DKIM-029**<br>DKIM Signing (Message Integrity) | No DKIM record found among probed selectors; test mode check not applicable. | Treat this as inconclusive unless message headers, vendor guidance, or known selectors confirm whether DKIM signing is enabled. |
| INFO | **VRD-DKIM-030**<br>DKIM Signing (Message Integrity) | No DKIM record found among probed selectors; key revocation check not applicable. | Treat this as inconclusive unless message headers, vendor guidance, or known selectors confirm whether DKIM signing is enabled. |
| INFO | **VRD-DKIM-031**<br>DKIM Signing (Message Integrity) | No DKIM record found among probed selectors; selector count cannot be evaluated. | Informational only: vendors may use more than one selector if they want easier key rotation. |
| INFO | **VRD-DKIM-032**<br>DKIM Signing (Message Integrity) | No DKIM record; provider cannot be identified. | Informational: Vendor appears to use a known email provider. Ensure they have enabled DKIM signing in that platform. |
| INFO | **VRD-DMARC-008**<br>DMARC Enforcement (Spoofing Exposure) | Relaxed alignment is the DMARC default. Absence of | Optional hardening only: the vendor may consider adkim=s and/or aspf=s if their mail flows support it. |

| STATUS | RULE | DETAILS | RECOMMENDATION |
|---|---|---|---|
| | | strict alignment is not, by itself, a finding. | |
| INFO | **VRD-INFRA-025**<br>Mail Infrastructure Hygiene | BIMI not detected. BIMI is optional and not a core security control. | Optional: vendor can publish BIMI (default._bimi) if they want visual brand indicators. |
| INFO | **VRD-INFRA-036**<br>Mail Infrastructure Hygiene | CAA record not detected. This is an informational hardening opportunity, not a substantive email-security finding. | Informational only: the vendor may publish CAA records to restrict which certificate authorities can issue certificates for the domain. |
| NA | **VRD-DKIM-027**<br>DKIM Signing (Message Integrity) | No DKIM record found; key strength cannot be evaluated. | Use DKIM keys appropriate to the algorithm in use. For RSA, prefer 2048-bit or stronger keys. Rotate all selectors, not just the primary. |
| NA | **VRD-REP-040**<br>Domain Reputation & Risk Signals | Data unavailable for this check (missing: vendor.reputation.domainAgeDays). | Exercise caution with new vendor domains. Request additional verification of the vendor's legitimacy. |
| NA | **VRD-REP-041**<br>Domain Reputation & Risk Signals | Data unavailable for this check (missing: vendor.reputation.domainAgeDays). | Domain age is acceptable but still relatively new. Standard vendor verification procedures are recommended. |

PASS **23 checks passed — No action required**

| | |
|---|---|
| **VRD-DMARC-001** | DMARC record found |
| **VRD-DMARC-002** | DMARC syntax appears valid |
| **VRD-DMARC-003** | DMARC policy tag (p) is present and valid |
| **VRD-DMARC-004** | DMARC policy is enforcing (quarantine/reject) |
| **VRD-DMARC-006** | DMARC pct is 100% (full enforcement) or not specified |
| **VRD-DMARC-007** | DMARC subdomain tag (sp) is present or main policy is strict |
| **VRD-DMARC-009** | Aggregate reporting (rua) appears enabled |
| **VRD-DMARC-043** | Subdomain DMARC policy is not weaker than the parent policy (or inherits the parent policy) |
| **VRD-INFRA-022** | MX record detected |
| **VRD-INFRA-023** | Multiple MX hosts detected, or known cloud provider with built-in redundancy |
| **VRD-INFRA-034** | MX records point to valid hostnames |
| **VRD-INFRA-035** | MX hostname resolves to a valid IP address |
| **VRD-INFRA-037** | MX indicates use of a known secure email provider (Google, Microsoft, Proofpoint, Mimecast, etc.) |
| **VRD-REP-039** | No adverse result was returned by the selected external corroboration signal used for this check. This does not guarantee the domain is safe or risk-free |
| **VRD-REP-042** | No adverse result was returned by the selected external reputation signal used for this check. This does not guarantee the domain is safe or risk-free |
| **VRD-SPF-010** | SPF record found |
| **VRD-SPF-011** | Single SPF record detected |
| **VRD-SPF-013** | SPF lookup count is within limits (<=10) |
| **VRD-SPF-014** | No deprecated 'ptr' mechanism detected |
| **VRD-SPF-015** | No multiple redirect= directives detected |
| **VRD-SPF-016** | SPF record parsed without critical errors |
| **VRD-SPF-017** | SPF ip4/ip6 syntax appears valid |
| **VRD-SPF-018** | SPF include count is reasonable |

# Disclaimer

**MOORLI VendorRiskDiagnostic** is an automated intelligence service provided by **MOORLI LLC** that evaluates the **public email security configuration** of internet domains. The risk scores, grades, and remediation recommendations in this report are generated by software algorithms using **external, non-intrusive analysis of public technical signals** and are provided solely for **informational and educational purposes**.

**External, non-intrusive analysis only.** This Service analyzes publicly available DNS records, lightweight public-web signals, authoritative registration context, and selected third-party reputation and threat-intelligence signals used as corroborating inputs. We do not send test emails, attempt authentication, access vendor systems, conduct penetration testing, or perform intrusive security testing of any kind.

**Provider-agnostic.** This Service is intended to be provider-agnostic and focuses on a domain's observable, publicly published configuration (e.g., SPF/DMARC/MTA-STS/DNSSEC). We do not provide opinions about, endorse, or certify any email service provider, DNS host, or cloud vendor. Any third-party product or brand names referenced are the property of their respective owners and are used only for identification.

**No professional advice.** MOORLI VendorRiskDiagnostic, its creators, and affiliates are not cybersecurity firms, managed security service providers (MSSPs), insurers, or legal professionals. We do not provide legal, regulatory, tax, insurance, or professional cybersecurity advice. You should consult qualified professionals as appropriate.

**No guarantee.** A "Low Risk" score does not guarantee that a vendor is immune to cyber attacks, nor does a "Critical" score guarantee a breach will occur. The information presented here should not be the sole basis for terminating vendor contracts or making financial decisions.

**Third-party signal limits.** MOORLI VendorRiskDiagnostic uses selected third-party reputation and threat-intelligence signals as corroborating inputs in its analysis of potentially malicious activity. These external sources are provided **"AS IS"** and are not perfect or exhaustive: some risky resources may not be identified, and some benign resources may be flagged in error. We do not redistribute raw third-party threat-intelligence data and instead use these signals as one factor within our own scoring and findings.

**Accuracy limits.** Data accuracy depends on the availability and propagation of public DNS records at the precise moment of the scan. Temporary DNS outages, propagation delays, registrar/host behavior, or third-party misconfigurations may affect results. MOORLI LLC makes no representations or warranties regarding the accuracy, reliability, or completeness of any data generated.

**AS-IS.** Reports are provided **"AS IS"** without warranty of any kind — express or implied — including but not limited to warranties of merchantability, fitness for a particular purpose, accuracy, or non-infringement.

**Limitation of liability.** To the fullest extent permitted by law, MOORLI LLC and its affiliates shall not be liable for any direct, indirect, incidental, consequential, special, punitive, or exemplary damages arising from the use of this report or reliance on its contents (including, but not limited to, lost profits, business interruption, or loss of programs/data). **In any event, MOORLI LLC's total aggregate liability for any claim related to the Service or any report shall not exceed the amount you paid for the specific audit/report giving rise to the claim.** Payment, refunds, and chargeback terms are governed by the Terms of Service; except where required by law, purchases are non-refundable once processing begins.

By using this product, you acknowledge and agree that you are solely responsible for validating all recommendations before implementation. Use of MOORLI VendorRiskDiagnostic constitutes acceptance of this Disclaimer and the accompanying Terms of Service and Privacy Policy.