VAIXUS
Technologies

ASR-2026-001

Infrastructure Assessment Report

Full Infrastructure Authentication Audit

Prepared for: [Sample Organization] (Synthetic Engagement)
Prepared by: Vaixus Technologies
Publication Date: June 25, 2026
Document Version: 1.0
Classification: Confidential Sample Deliverable

LABORATORY-ENGINEERED CONSULTING SIMULATION

This report is a fictional, laboratory-generated case study prepared for portfolio and methodology-demonstration purposes. It does not describe a real client, a real organization, or an actual engagement.

Synthetic Demonstration Notice

This report is a representative demonstration of the Vaixus assessment methodology. Organization names, domains, identifiers, and evidence samples have been synthesized to illustrate a typical enterprise engagement. Representative evidence shown throughout this document does not originate from an actual client. The assessment process, report structure, and technical reasoning reflect the exact standards used during production consulting engagements.

Document Control

Field	Value
Document Title	ASR-2026-001 — Infrastructure Assessment Report
Document Version	1.0
Publication Date	June 25, 2026
Prepared By	Vaixus Technologies
Review Status	Final — Approved for Publication
Classification	Confidential Sample Deliverable
Engagement Type	Laboratory-Engineered Consulting Simulation

Revision History

Version	Date	Author	Summary of Changes
1.0	June 25, 2026	Soorya S V	Final release following technical assessment.

Table of Contents

1. Engagement Information

Field	Value
Client Company	[Sample Organization]
Primary Contact	Chief Information Officer (CIO)
Primary Domain	[Demonstration Domain]
Assessment Type	Full Infrastructure Authentication Audit
Assessment Date	June 25, 2026
Consultant	Soorya S V, Principal Consultant

2. Assessment Objectives

Objective	Description
Current State Assessment	Establish the current state of the client’s email infrastructure
Infrastructure Inventory	Document all domains, subdomains, mail platforms, and sending systems
Authentication Analysis	Assess SPF, DKIM, DMARC, MX, PTR, MTA-STS, and TLS-RPT configurations
Risk Identification	Identify authentication and infrastructure risks with supporting evidence
Evidence Collection	Document technical evidence for each finding
Readiness Evaluation	Determine readiness for remediation activities

3. Scope of Assessment

In Scope

- Domains and subdomains
- DNS configuration: SPF, DKIM, DMARC, MX, PTR, MTA-STS, TLS-RPT
- Primary mail platform (e.g., Google Workspace, Microsoft 365)
- Third-party sending platforms and email service providers
- Publicly observable infrastructure and sending sources
- Authentication protocol configuration and alignment
- Reporting and monitoring configuration

Out of Scope

- Email content review and marketing strategy
- Customer databases, CRM data, and list hygiene
- Revenue forecasting and deliverability guarantees
- Penetration testing
- Compliance certification and legal advice

4. Executive Findings Snapshot

ID	Finding	Severity	Business Impact	Priority	Status
F-001	SPF 10-Lookup Limit Exceeded (11/10)	Critical	Elevated risk of message rejection by recipient gateways	P1	Open
F-002	DMARC Policy in Monitoring (p=none)	High	Domain presents elevated spoofing and phishing exposure	P1	Open
F-003	Salesforce DKIM Not Enabled	High	CRM-originated messages may experience reduced inbox placement	P2	Open
F-004	Missing MTA-STS Policy	Medium	Mail transit vulnerable to TLS downgrade attacks	P3	Open

Risk Classification Methodology

Field	Value
Critical	Authentication failure causing significant business interruption.
High	Likely deliverability degradation or dependency risk.
Medium	Configuration weaknesses requiring remediation.
Low	Improvement opportunities with minimal business impact.

Risk Heat Matrix

Likelihood \ Impact	Low Impact	Medium Impact	High Impact
High Likelihood	Medium	High	Critical
Medium Likelihood	Low	Medium	High
Low Likelihood	Low	Low	Medium

5. Environment Inventory

5.1 Domain: [Demonstration Domain]

Field	Value
Registrar & DNS Provider	Cloudflare Enterprise
Primary Mail Platform	Google Workspace
Third-Party Platforms	Salesforce, SendGrid, Mailchimp
Domain Purpose	Primary Corporate Communications & Marketing

6. Authentication Assessment

METHODOLOGY — All authentication assessments use publicly observable DNS records. Evidence is in Appendix A. Each finding below evaluates technical risk, business impact, and required remediation.

F-001 — SPF Assessment: 10-Lookup Limit Exceeded

Severity	**Critical**
Category	Protocol Configuration
Reference	Lookup Count: 11 of 10 | Alignment Status: Misaligned

Evidence.

The SPF record contains multiple recursive include mechanisms for legacy third-party tools, pushing the DNS lookup count to 11. Reference DNS output in Appendix A. The extracted TXT record reveals an overloaded architecture:

```
v=spf1 include:_spf.google.com include:sendgrid.net include:_spf.salesforce.com
include:servers.mcsv.net ~all
```

Technical Analysis.

This configuration significantly increases the likelihood of an SPF PermError during recipient evaluation. It fundamentally breaks the RFC 7208 standard by demanding too many recursive DNS queries from the receiving mail server.

Business Impact.

Authentication failures may reduce inbox placement for critical business communications, depending on strict recipient gateway policies.

Recommendation.

Evaluate SPF restructuring through controlled flattening or architectural simplification while preserving authorized sending sources.

Verification Method.

Post-implementation DNS evaluation using CLI diagnostic tools to ensure lookup count is strictly ≤ 10.

F-002 — DKIM Assessment: Salesforce Not Enabled

Severity	**High**
Category	Deliverability
Reference	Selectors: google, s1, sf1 | Key Length: 2048/1024 bits

Evidence.

Google Workspace and SendGrid are actively signing with aligned DKIM keys. The Salesforce CNAME records are published in DNS, but cryptographic signing has not been activated within the Salesforce console. DNS queries returned valid public keys for 'google' and 's1', however, test email headers generated via Salesforce lacked the required DKIM-Signature block.

Technical Analysis.

Emails originating from the Salesforce CRM fail cryptographic validation at the recipient level because the platform is not actively attaching cryptographic signatures to outbound mail.

Business Impact.

Sales and automated billing emails generated via the CRM are highly likely to be quarantined by strict spam filters.

Recommendation.

Activate DKIM signing within the Salesforce administrative console and verify cryptographic alignment.

Verification Method.

Send test messages from all platforms and verify passing DKIM signatures in raw email headers.

F-003 — DMARC Assessment: Policy in Monitoring

Severity	**High**
Category	Security
Reference	Enforcement Readiness: Conditionally Ready | Alignment: Partially Aligned

Evidence.

DMARC is currently stalled in monitoring mode (p=none) for the primary domain, though subdomains are protected (sp=quarantine). Aggregate reporting (rua) is actively collecting data. The current DNS TXT record for _dmarc.[Demonstration Domain]:

```
v=DMARC1; p=none; sp=quarantine; rua=mailto:reports@[REDACTED];
```

Technical Analysis.

Because the primary policy is p=none, malicious actors can freely spoof the root domain. Recipient servers are explicitly instructed to take no action on unauthorized mail.

Business Impact.

The domain presents elevated spoofing and phishing exposure. Malicious actors can easily impersonate the brand in attacks targeting clients and vendors.

Recommendation.

Achieve 100% DKIM alignment across all authorized vendors, analyze the aggregate reports to confirm no legitimate mail is failing, and systematically escalate the policy to p=quarantine and ultimately p=reject.

Verification Method.

Query the _dmarc TXT record to confirm updated policy enforcement tags.

6.4 Infrastructure Strengths (Positive Findings)

- Google Workspace MX: MX records are optimally configured with correct priorities, ensuring mail routing redundancy.
- DNSSEC: Domain Name System Security Extensions (DNSSEC) are actively enabled, preventing DNS spoofing on the root domain.
- Cloudflare DNS: Enterprise-grade DNS hosting ensures high availability and rapid record propagation.

7. Sending Infrastructure Mapping

Platform	Purpose	Auth Method	Sending Domain	Dependencies	Risk
Google Workspace	Corporate Email	SPF / DKIM	[Demonstration Domain]	None	Low
SendGrid	Transactional	SPF / DKIM	[Demonstration Domain]	None	Low
Salesforce	CRM	None	[Demonstration Domain]	DNS DKIM	High
Mailchimp	Marketing	None	[Demonstration Domain]	DNS DKIM / SPF	High

8. Risk Register

ID	Category	Finding	Severity	Priority	Status
F-001	Protocol	SPF Lookup Limit Exceeded	Critical	P1	Open
F-002	Security	DMARC Enforcement Lacking	High	P1	Open
F-003	Deliverability	Salesforce DKIM Inactive	High	P2	Open

9. Prioritized Recommendations

9.1 Priority 1 – Immediate Action Required

PRIORITY 1 NOTE — Findings in this category require immediate attention. Deferral increases operational and authentication risk.

F-001 – Resolve SPF Lookup Limit

Issue: The SPF record requires 11 DNS lookups, breaking the RFC 7208 standard.

Why It Matters: Critical business operations are experiencing random email delivery failures.

Recommended Action: Migrate legacy include statements to a flattened infrastructure or utilize SPF delegation.

Dependencies: Confirmation of active sending sources.

Risk If Ignored: Elevated risk of message rejection by recipient gateways.

Validation: SPF lookup count evaluates to ≤ 10.

F-002 – Secure Salesforce DKIM Alignment

Issue: Salesforce is sending unauthenticated mail on behalf of the primary domain.

Why It Matters: Sales and billing emails are landing in recipient spam folders.

Recommended Action: Provision DKIM keys within the Salesforce console and publish the corresponding CNAME records in Cloudflare.

Dependencies: Administrator access to the Salesforce platform.

Risk If Ignored: Continued deliverability degradation for CRM communications.

Validation: Successful DKIM signing verified via raw email headers.

10. Assumptions and Limitations

- Assessment limited to publicly observable DNS and infrastructure data only
- Unknown third-party dependencies: not all sending platforms may be identified
- Snapshot-in-time: DNS and infrastructure conditions may change after the assessment date
- DNS propagation limitations: recent changes may not be fully propagated at time of assessment
- Provider behaviour is outside Vaixus control; third-party configurations may change independently
- Infrastructure changes occurring after assessment completion are not reflected in this report

11. Overall Infrastructure Status

NEEDS IMPROVEMENT

Status	Assessment
Needs Improvement	High Risk Profile. The combination of an SPF PermError and a lack of primary DMARC enforcement places the domain at elevated risk for both deliverability degradation and brand impersonation.
Readiness	Ready for Remediation. The current inventory of sending platforms is fully mapped and baseline reporting is active.
Next Step	Proceed to structured remediation.

12. Consultant Conclusion

Infrastructure Summary

The infrastructure for the primary domain exhibits common scale-related architectural fractures. While foundational security measures (DNSSEC, Google Workspace MX routing) are excellently configured, the unmanaged addition of third-party marketing and CRM vendors has bloated the SPF record beyond RFC operational limits.

Key Risks

The immediate operational threat is the SPF limit breach, which degrades day-to-day corporate communication reliability. Furthermore, stalling the DMARC migration at p=none leaves the primary brand exposed to direct spoofing attacks.

Remediation Readiness Opinion

Based on the assessment scope, sufficient information and aggregate data have been collected to begin a structured remediation engagement. No further discovery is required.

INDEPENDENT STATEMENT — This assessment represents an independent technical opinion based solely on observable infrastructure conditions at the time of assessment. Vaixus does not guarantee future provider behaviour, inbox placement, business outcomes, or future infrastructure conditions.

RECOMMENDATION — Proceed with Remediation.

Appendices

Appendix A – DNS Output

Representative DNS output redacted for demonstration. Example artifact of SPF validation failure:

```
; <<>> DiG 9.16.1-Ubuntu <<>> TXT [Demonstration Domain]
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61234
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
[Demonstration Domain]. 300 IN TXT "v=spf1 include:_spf.google.com include:sendgrid.net
include:_spf.salesforce.com include:servers.mcsv.net ~all"
```

Appendix B – Screenshots

[Authentication validation screenshots and console configurations withheld from demonstration sample.]

Appendix C – DMARC Reports

Aggregate DMARC reporting excerpts removed. Representative demonstration artifact illustrating a typical Salesforce DKIM alignment failure:

```
  "record": {
    "row": {
      "source_ip": "[IP Redacted]",
      "count": 142,
      "policy_evaluated": {
        "disposition": "none",
        "dkim": "fail",
        "spf": "pass"
      }
    }
```

Appendix D – Evidence Register

Evidence ID	Type	Description	Collection Date	Reference
E-001	[DNS Output]	SPF/DKIM/DMARC TXT Queries	June 25, 2026	Appendix A
E-002	[Screenshot]	Salesforce CRM DNS Config	June 25, 2026	Appendix B
E-003	[DMARC Report]	RUA Aggregate XML Data	June 25, 2026	Appendix C