

VANCESENTINENTAL — DELIVERABILITY AUDIT

SAMPLE REPORT — illustrative example only. The company, domain, and findings below are fictitious and shown to demonstrate the report format a real Deliverability Audit produces.

Prepared for: Sample Co. (example-sender.com)
Engagement: Deliverability Audit
Report date: [Sample — dates reflect your actual engagement]
Domains reviewed: example-sender.com, mail.example-sender.com

EXECUTIVE SUMMARY

example-sender.com is authenticating mail correctly on the checks that matter most day-to-day, but two issues are quietly capping deliverability and are worth fixing before they cause a visible drop in reply rates: the SPF record is one lookup away from exceeding RFC 7208's 10-lookup limit, and DMARC is still sitting at p=none — meaning it's watching for spoofing but not stopping any of it. Neither is an emergency. Both are the kind of thing that looks fine for months and then breaks all at once, usually right after a new email tool gets added.

Both are addressed in Prioritized Recommendations below, ranked by how much they'd cost you if left alone.

FINDINGS

Check	Status	What we found
SPF	WARNING	9 of 10 allowed DNS lookups in use. One more include (a new tool, a forwarding service) pushes this into a silent permerror — mail starts failing SPF with no visible error on your end.
DKIM	PASS	Valid signature found under the google selector, aligned correctly with the sending domain.
DMARC	WARNING	Record present at p=none. Monitoring only — spoofed mail using your domain is not being blocked or quarantined.
MX	PASS	Two mail exchangers configured correctly, priorities set as expected.
Blacklist	PASS	Sending IP not listed on Spamhaus ZEN, SpamCop, or Barracuda at time of check.

PRIORITIZED RECOMMENDATIONS

1. Reduce SPF lookups now, not after it breaks.

Consolidate or flatten the includes currently in use — this is typically a 15-minute DNS change. Waiting until a new tool pushes the count over 10 means mail silently starts failing for an unpredictable subset of recipients, which is far harder to diagnose after the fact than to prevent now.

2. Move DMARC from p=none to p=quarantine over the next 2-4 weeks.

Confirm every legitimate sending source is correctly aligned first (this audit found none currently misaligned), then move to quarantine, then reject. Staying at p=none indefinitely means the record exists but isn't actually protecting the domain from spoofing.

3. Re-run both checks after the SPF change.

A lookup-count fix is easy to get subtly wrong. A follow-up check confirms the new record is both under the limit and still passing for every real sending source.

WHAT THIS AUDIT DOES NOT COVER

This is a diagnostic-only engagement — no changes were made to example-sender.com's DNS. A Hardening Sprint covers the fix-and-verify version of this same audit; ongoing VanceSentinental monitoring catches the moment either of these — or anything else — changes state again after they're fixed.

This sample was generated to show the exact format and depth of a real Deliverability Audit report. Your report will reflect your actual domains, actual findings, and actual recommendations.