What we checked before launching Client name

Before the first send, Your agency ran an independent infrastructure audit on client-domain.com. It reads public records only: DNS, the domain registry, Certificate Transparency logs, and public blocklists. It never needs a mailbox password or a sending-platform key.

75 checks across four asset types

57

Sending domains

Authentication, routing, TLS, reputation, registration, and observed sender history.

8

Tracking domains

Resolution, certificate validity, redirect behaviour, and separation from the sending domain.

7

SMTP egress paths

Reverse DNS, HELO, banner, TLS, and blocklist exposure for the IP you actually send from.

3

Inboxes

Alignment with the sending domain and the authentication the receiver will see.

Every finding is evidence-backed: the record we read, the value it holds, and the value it should hold. You can verify any of it yourself with free public tools.

The verdict for client-domain.com

Ready

No blocker was found across the infrastructure we can verify from public records.

What happens next

Launch as planned. Monitoring stays on so a record change is caught the day it happens, not the week replies stop.

The full report

Every check, its result, and its evidence is in the shareable report. It opens in a browser with no login.

`https://outboundqa.com/r/...`

A verdict describes how this domain is configured and what public reputation it carries. It is not a prediction of inbox placement, which also depends on list quality, message copy, volume, and mailbox provider behaviour that no public source exposes.

What launching with unresolved blockers costs

A blocker is cheap to fix and expensive to ignore. The asymmetry is the whole argument for checking before the first send rather than after the reply rate drops.

A burned domain does not come back

Reputation attaches to the domain and to the sending IP behind it. Once receivers have learned to distrust it, warming it again takes longer than registering a new one, and the new one starts from zero.

Replacement is the real cost, not the fix

A record change takes minutes. Replacing a burned domain means a new registration, a new warmup window, new inboxes, and a paused campaign while all of it happens.

The damage is not contained to one domain

Sending domains that share a root, an IP, or a mailbox tenant are evaluated together. One bad sender can pull its neighbours down with it.

You find out late

Reply rate is the last signal to move and the noisiest one. By the time a campaign looks wrong, weeks of sending have already been recorded against the domain.

Our recommendation

Launch as planned. Monitoring stays on so a record change is caught the day it happens, not the week replies stop.