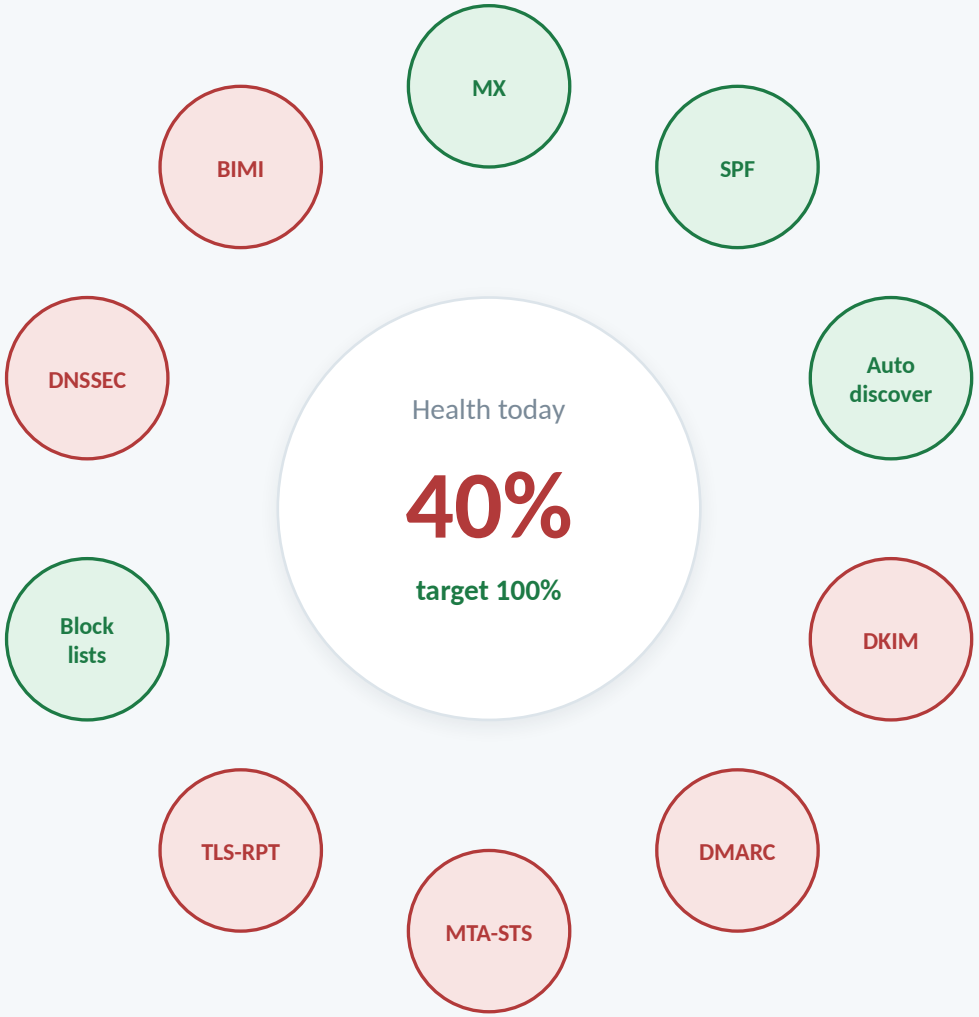
Ability

abilityglobal.io
Domain Health Program

Diagnosis, the fix plan, and the path to a perfect-health domain that is ready for bulk email.

Live DNS audit | 16 September 2026



4 / 10	10 / 10	3
health checks passing today	target in 45 days	root causes confirmed

CONTENTS

What this program covers

Three parts: find out exactly why mail lands in spam, fix it to perfect health, then make the domain ready for bulk email.

PART 1

Diagnosis

- What we found in live DNS
- Symptom to root-cause tree
- Evidence to collect inside the tenant
- Risk ranking

PART 2

Fix to perfect

- Seven-phase plan with dates
- Exact DNS record sheet
- Microsoft 365 hardening
- DMARC journey to reject
- Test matrix and pass marks

PART 3

Bulk readiness

- What "bulk" means for Ability
- Subdomain architecture
- Bulk platform setup
- Volume ramp and list rules
- Monitoring and owners

Ability

PART 1

Diagnosis

Why mail from abilityglobal.io lands in spam, based on live records and what still needs checking inside Microsoft 365.

LIVE DNS AUDIT

What receiving servers see today

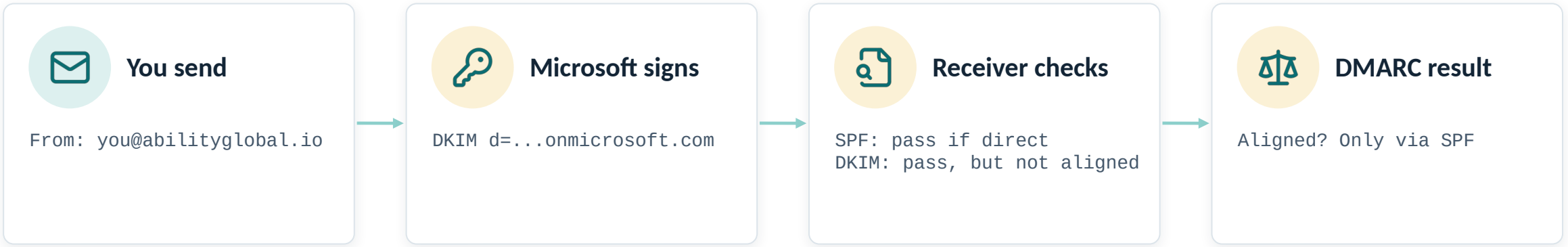
Queried through public resolvers on 16 Sep 2026. Green passes, amber needs work, red is broken.

NOTE	**DNS host**	`Cloudflare (tessa / clyde)`	Registrar is GoDaddy. All edits happen in Cloudflare.
PASS	**MX**	`abilityglobal-io.mail.protection.outlook.com`	Microsoft 365 receives mail correctly.
WEAK	**SPF**	`v=spf1 include:spf.protection.outlook.com ~all`	Valid, 1 include. Soft fail ~all; other senders not listed.
FAIL	**DKIM**	`selector1 / selector2 not found`	Custom DKIM not enabled. No aligned signature.
WEAK	**DMARC**	`p=quarantine; adkim=r; aspf=r; rua=...@onsecureserver.net`	Reports go to a GoDaddy service. No monitoring.
FAIL	**MTA-STS / TLS-RPT**	`Not published`	No enforced TLS policy for inbound mail.
FAIL	**DNSSEC**	`No DS record at .io`	Zone not signed.
FAIL	**BIMI**	`Not published`	No logo in inbox. Needs DMARC enforcement first.
WEAK	**Web records**	`apex A 5.9.113.156 direct; www via Cloudflare proxy`	Origin server exposed; inconsistent setup.
NOTE	**Blocklists**	`SURBL clean`	Spamhaus and URIBL need an MXToolbox check.

THE CORE PROBLEM

Why your own mail fails DMARC

DMARC needs SPF or DKIM to pass AND match your From domain. Today only SPF can, and forwarding breaks it.



Path A: sent directly to Gmail or Outlook

SPF passes and aligns, so DMARC passes. But inbox providers now expect DKIM too, and a DKIM-less sender with no history is scored as low trust. Result: often junk for new contacts.

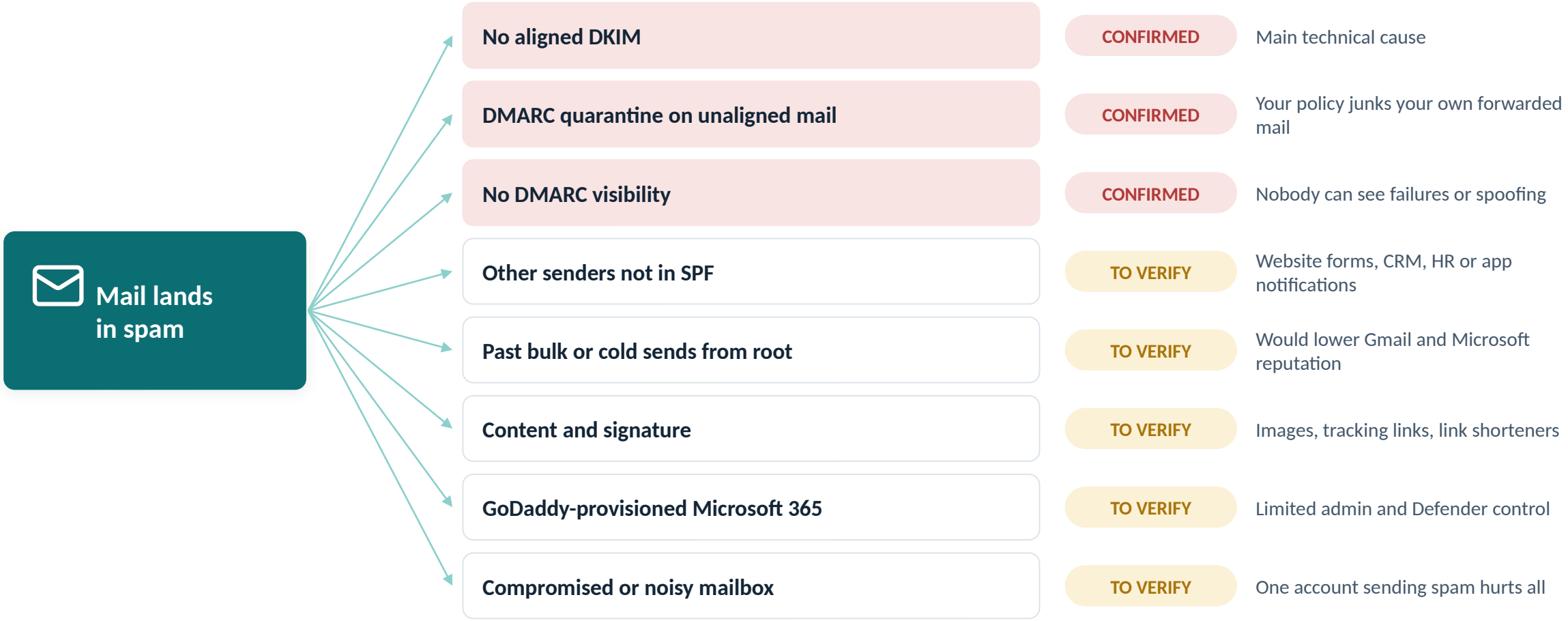
Path B: forwarded, relayed or via a gateway

SPF breaks (new sending IP), DKIM is not aligned, so DMARC fails. Your own p=quarantine policy then instructs the receiver to put the email in spam. Common with enterprise and bank recipients.

ROOT-CAUSE TREE

Symptom to causes, confirmed and suspected

Confirmed from live DNS. Suspected items need evidence from the tenant, Postmaster Tools and past sending.



DIAGNOSIS CHECKLIST

Evidence to collect in the first 48 hours

Some causes cannot be seen from outside. These checks close every open question.

Message headers

Send to a Gmail and Outlook.com test account. Read Authentication-Results for spf, dkim, dmarc and the X-Microsoft-Antispam SCL score.

Google Postmaster Tools

Verify the domain. Check spam rate, compliance status and authentication graphs once data appears.

Microsoft Defender

Restricted users list, outbound spam alerts, message trace for last 30 days of external volume per mailbox.

Blocklists

MXToolbox Blacklist + Domain Health, Spamhaus DBL lookup for the domain.

Sender inventory

List every system sending as @abilityglobal.io: website, CRM, Novara HR, OrviQ, invoicing, HR tools.

Tenant ownership

Is Microsoft 365 billed through GoDaddy? Can admins reach Defender and Exchange admin centers fully?

Sending history

Any past newsletters, mass mails or cold campaigns from the root domain? Dates and volumes.

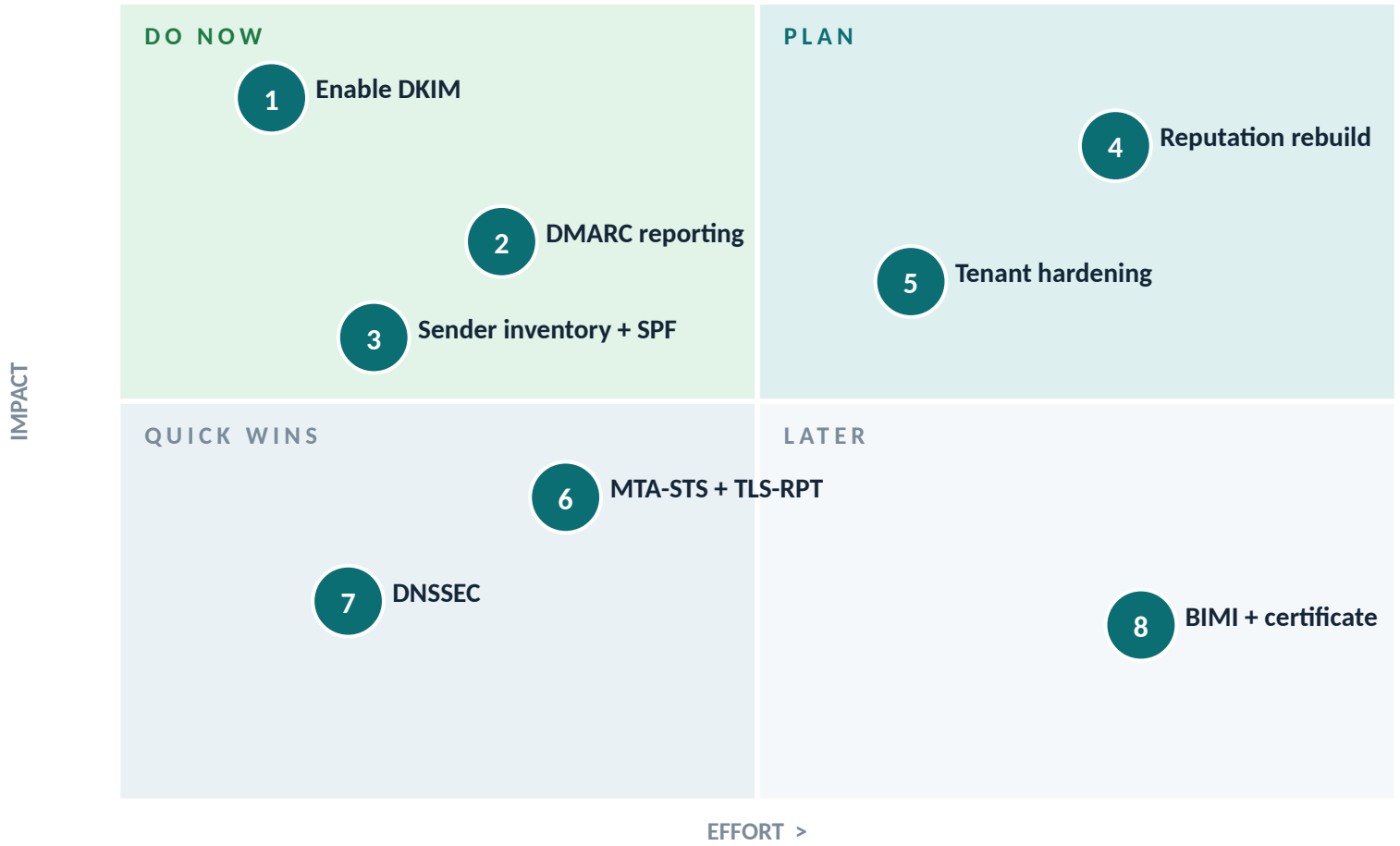
Content audit

Signatures: images, tracking pixels, banners, shortened links, legal disclaimers as images.

RISK RANKING

Impact versus effort to fix

Start in the top-left: highest impact, least effort.



TOP FIVE

1. Enable DKIM

20 minutes, removes the main cause

2. DMARC reporting

Turns on visibility for every sender

3. Sender inventory

Stops silent SPF failures

4. Reputation rebuild

Weeks of clean, engaged mail

5. Tenant hardening

Protects against compromised accounts

Ability

PART 2

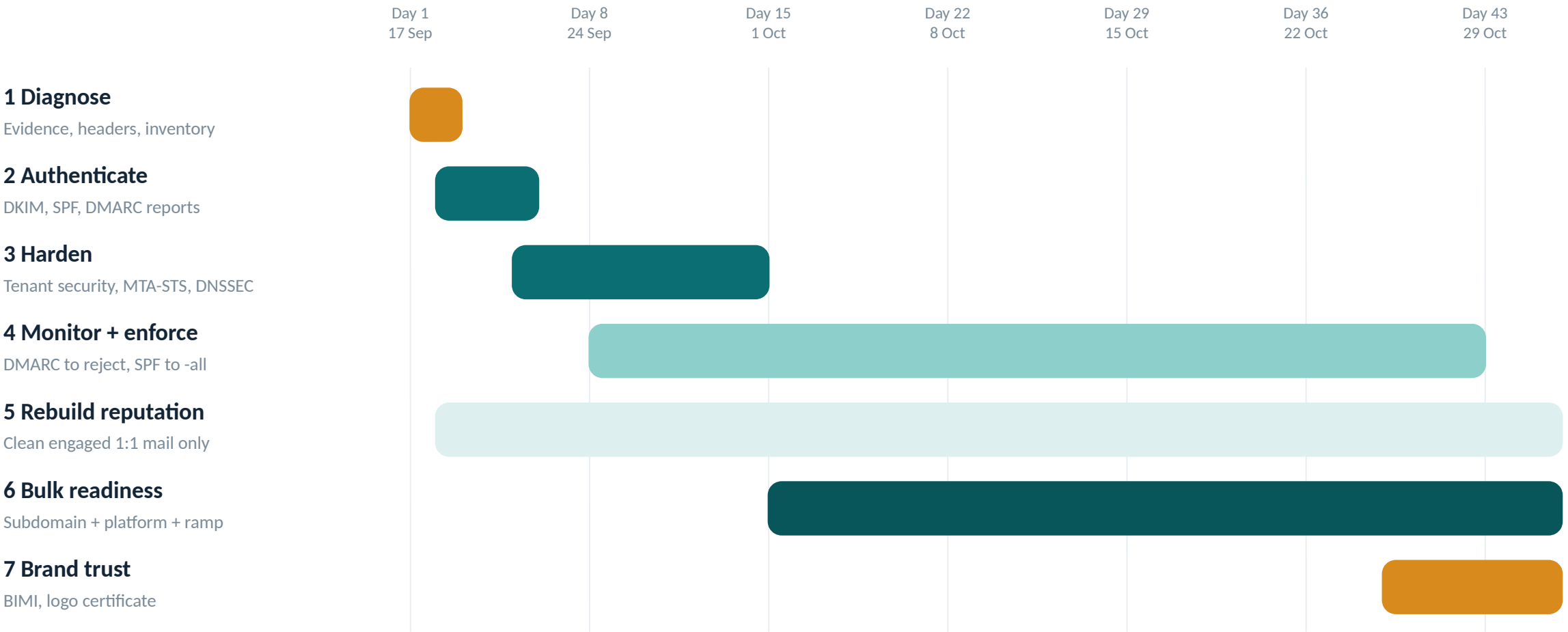
Fix to perfect

Seven phases take abilityglobal.io from 4 of 10 to a full 10 of 10 health score in 45 days.

FIX PLAN

Seven phases, 45 days, one owner each

Phases overlap. Nothing in phase 6 starts until phases 1 to 4 pass.



Diagnose, then authenticate

The fastest, highest-impact work. Owner: Microsoft 365 admin with Cloudflare access.

1	**Collect evidence**	Run the 8-point checklist; save headers and screenshots	Day 1 to 2
2	**Freeze bulk from root**	No newsletters, mass mail or cold sends from abilityglobal.io	Day 1
3	**Enable DKIM**	Defender portal: Email authentication settings > DKIM > abilityglobal.io > enable, copy CNAMEs	Day 1
4	**Publish DKIM CNAMEs**	Cloudflare, DNS only (grey cloud), TTL 3600; toggle signing on; confirm 2048-bit	Day 1
5	**DMARC reporting**	Create a DMARC monitor account; change rua; keep p=quarantine	Day 2
6	**Sender inventory**	Every system that sends as the domain gets SPF include + DKIM, or moves to a subdomain	Day 2 to 5
7	**Verify**	Headers show dkim=pass header.d=abilityglobal.io and dmarc=pass	Day 3 to 5

EXIT CRITERIA

- DKIM status: Signing
- dkim=pass, aligned
- dmarc=pass
- Reports arriving
- Every sender listed

RECORD SHEET

The perfect-health DNS zone for abilityglobal.io

Enter in Cloudflare. Values in angle brackets come from Microsoft, your DMARC monitor or your policy host.

TYPE	HOST	VALUE	STAGE
MX	@	0 abilityglobal-io.mail.protection.outlook.com	keep
TXT	@	v=spf1 include:spf.protection.outlook.com <other senders> -all	day 30
CNAME	selector1._domainkey	selector1-abilityglobal-io._domainkey.<tenant>.<x>-v1.dkim.mail.microsoft	day 1
CNAME	selector2._domainkey	selector2-abilityglobal-io._domainkey.<tenant>.<x>-v1.dkim.mail.microsoft	day 1
TXT	_dmarc	v=DMARC1; p=quarantine; rua=mailto:<monitor>; adkim=r; aspf=r; fo=1	day 2
TXT	_dmarc	v=DMARC1; p=reject; sp=reject; rua=mailto:<monitor>; adkim=r; aspf=r; fo=1	day 30 to 45
TXT	_mta-sts	v=STSv1; id=20260920	day 7
CNAME	mta-sts	<policy host> (serves mode: testing, then enforce)	day 7
TXT	_smtp._tls	v=TLSRPTv1; rua=mailto:<monitor>	day 7
DS	(at registrar)	Enable DNSSEC in Cloudflare, add DS at GoDaddy	day 10
TXT	default._bimi	v=BIMI1; l=https://<host>/ability.svg; a=https://<host>/vmc.pem	day 45

Harden the Microsoft 365 tenant

A single compromised mailbox can burn the domain overnight. These controls stop that.

Identity

- MFA for every user, no exceptions
- Block legacy authentication
- Disable SMTP AUTH except named service accounts

Outbound spam policy

- Set per-user external limits (for example 500/hour, 1,000/day)
- Alert admins when a user is restricted
- Block automatic external forwarding

Monitoring

- Review Restricted users weekly
- Alert on unusual outbound volume
- Message trace export monthly

Tenant control

- Confirm full admin access to Defender and Exchange
- If billed via GoDaddy with limited control, move to a direct Microsoft tenant
- Remove stale mailboxes and shared inbox rules

Transport security and web trust

The layer most domains skip. Banks and enterprise security gateways notice.

MTA-STS
Forces other servers to deliver mail to you over verified TLS. Host policy file, start in testing, move to enforce after 14 days of clean TLS reports.

TLS-RPT
Daily reports of TLS failures when others send to you. Pairs with MTA-STS.

DNSSEC
Signs your DNS so records cannot be spoofed. One click in Cloudflare, then add the DS record at GoDaddy.

Web consistency
Proxy apex and www the same way through Cloudflare, HTTPS everywhere, redirect apex to www or reverse.

Trust pages
Business address in footer, privacy notice, terms, contact page. Receivers and people both check.

HOW MTA-STS WORKS

Sender server
looks up _mta-sts

↓

Fetches policy
mta-sts.abilityglobal.io

↓

Checks MX + TLS cert
matches policy

↓

Delivers encrypted
or refuses if tampered

Ability

The DMARC journey to reject

Each step moves only when reports show every legitimate sender passing aligned.

Today

`p=quarantine`

no DKIM, no visibility

Day 2

`p=quarantine + rua`

reports flowing to monitor

Day 14

`100% aligned`

all senders fixed, spoofing visible

Day 30

`SPF -all`

hard fail for unlisted IPs

Day 30 to 45

`p=reject; sp=reject`

spoofed mail refused

Rollback rule: if a legitimate source starts failing after reject, drop back to quarantine for that week, fix the source, then return to reject.

PHASE 5 | DAYS 1 TO 45

Rebuild sender reputation

Authentication gets you through the door. Reputation keeps you in the inbox.

DO

- Only person-to-person mail from abilityglobal.io
- Start threads with people who reply: clients, partners, team
- Ask frequent contacts to move you out of junk and reply
- Plain signatures: text, no image banners or tracking
- Links only to abilityglobal.io, never shorteners
- Remove inactive or bouncing addresses from CRM sync

DON'T

- Newsletters or mass mail from Outlook
- Cold outreach from the root domain
- BCC blasts to large lists
- Attachments to new contacts (send links instead)
- Open-tracking pixels in personal mail
- Auto-forwarding all mail to external inboxes

VERIFICATION

Test matrix and pass marks

Run at the end of each phase and weekly after. Every row must be green to call the domain perfect.

mail-tester.com	Overall score	10 / 10
Message headers (Gmail, Outlook)	spf, dkim, dmarc	all pass, DKIM d=abilityglobal.io
MXToolbox Domain Health	Errors and warnings	0 errors, 0 warnings
MXToolbox Blacklist + Spamhaus DBL	Listings	0
Google Postmaster Tools	Spam rate | compliance	under 0.1% | all pass
DMARC monitor	Aligned pass rate	99%+ of legitimate volume
TLS-RPT reports	Failed sessions	0 over 14 days
Hardenize or internet.nl mail test	Modern standards	all green
Seed inbox placement	Primary inbox rate	90%+

Ability

PART 3

Bulk readiness

Perfect health protects the brand. This part makes large-volume sending safe without putting abilityglobal.io at risk.

DEFINITIONS

Three kinds of bulk email, three homes

Mixing them on one domain is how brands end up in spam. Each stream gets its own reputation lane.

Opt-in marketing

Newsletters, product launches (OrviQ, Novara HR), event invites, client updates

SENDS FROM

`news.abilityglobal.io`

Bulk email platform

Transactional

Password resets, HR and GRC platform notifications, invoices, alerts

SENDS FROM

`notify.abilityglobal.io`

Transactional sender

Cold outreach

First-touch prospecting emails to people who have not opted in

SENDS FROM

`Separate sending domains`

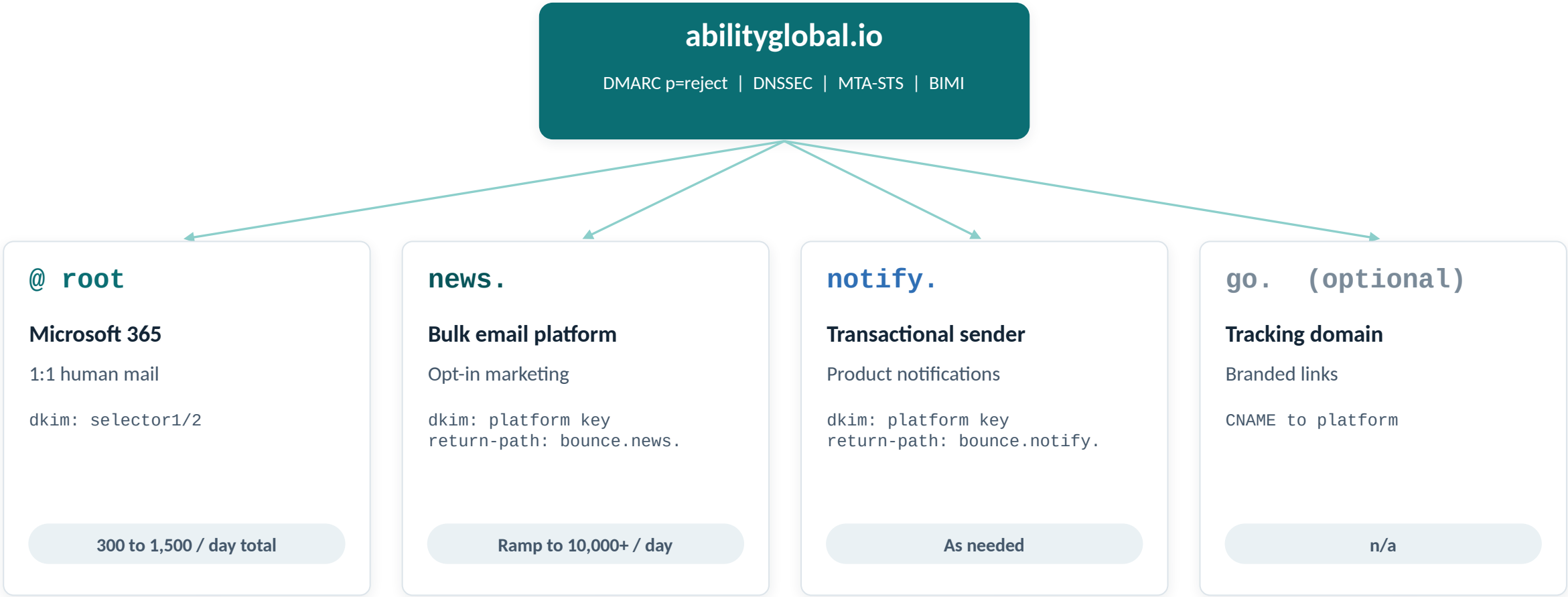
Email Outreach Engine plan

Never from Outlook mailboxes on abilityglobal.io: Microsoft 365 is built for person-to-person mail, not bulk. Use a dedicated platform for volume.

ARCHITECTURE

One brand, separated reputation lanes

Each subdomain has its own SPF, DKIM and bounce domain, all aligned under the abilityglobal.io DMARC policy.



Configure the news. subdomain for bulk

Any reputable bulk platform works (for example Brevo, SendGrid, Mailgun, Amazon SES, Postmark broadcast). These settings are what matter.

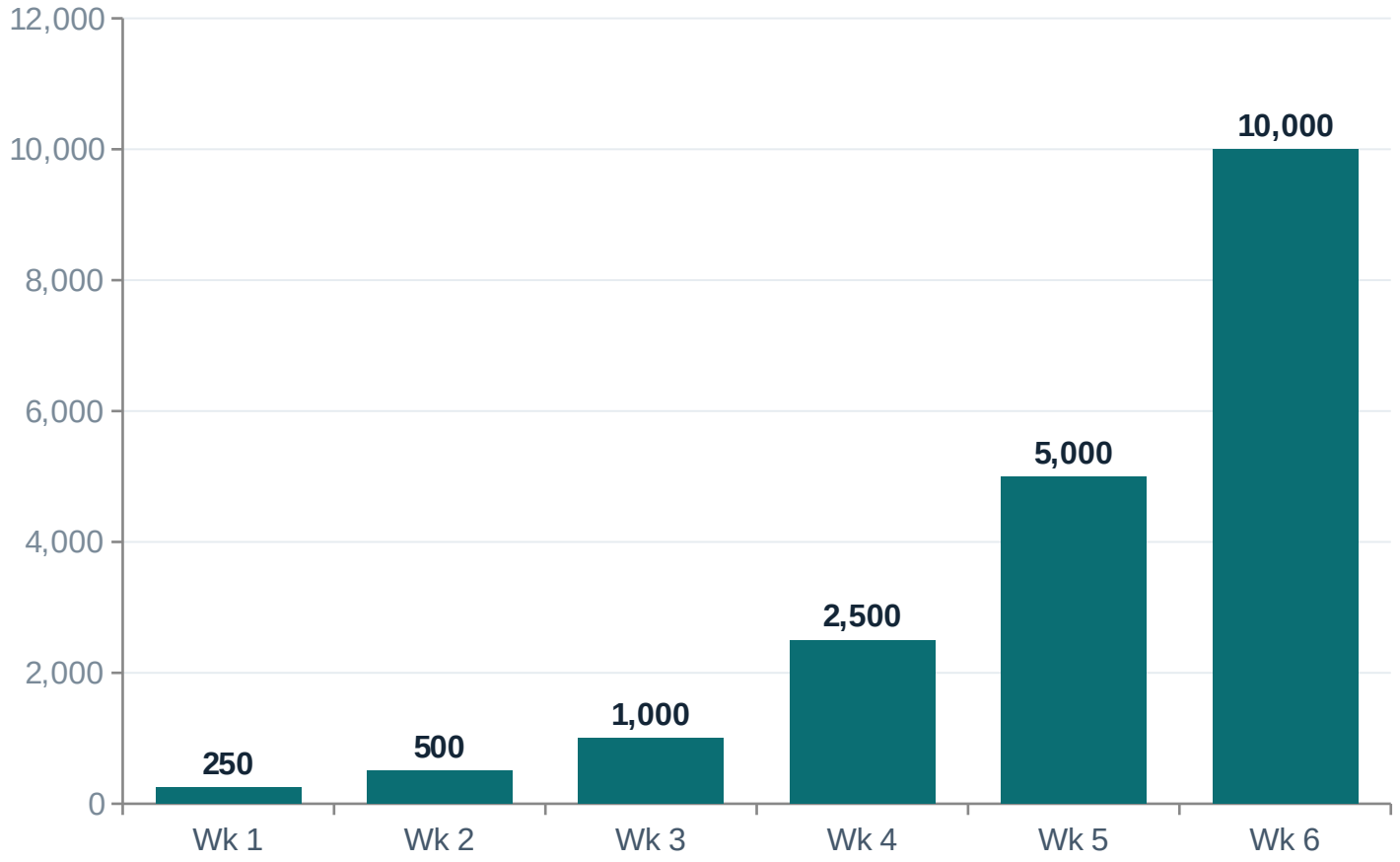
1. **Add subdomain**
   Authenticate news.abilityglobal.io in the platform
2. **DKIM 2048-bit**
   Platform DKIM CNAMEs, signing as d=news.abilityglobal.io
3. **Custom return-path**
   bounce.news.abilityglobal.io so SPF aligns
4. **SPF for subdomain**
   v=spf1 include:<platform> -all on the bounce host
5. **Branded tracking**
   go.abilityglobal.io, HTTPS, or tracking off
6. **One-click unsubscribe**
   List-Unsubscribe + List-Unsubscribe-Post (RFC 8058)
7. **Suppression sync**
   Unsubscribes and bounces shared with CRM daily
8. **Feedback loops**
   Microsoft JMRP and SNDS, Yahoo CFL where offered

Shared IP is correct below roughly 100,000 emails a month. A dedicated IP only helps with steady, larger volume.

VOLUME RAMP

Warm the bulk lane with your best contacts first

Engaged recipients first build positive signals. Step up only when the week passes every KPI.



Wk 1 to 2

Clients, partners, people who replied in 90 days

Wk 3 to 4

Opted-in contacts engaged in 6 months

Wk 5 to 6

All confirmed opt-ins, re-verified

Never

Purchased, scraped or unverified lists

Ability

What goes into every bulk send

Good lists and honest content decide placement more than any DNS record.

Consent

- Double opt-in for new subscribers
- Record source and date for every contact
- Clear preference centre

Hygiene

- Verify lists older than 30 days
- Sunset contacts with no engagement in 6 months
- Remove hard bounces instantly

Content

- Text-to-image balance, alt text, no image-only mails
- Consistent From name: "Ability" or a real person
- Visible address and unsubscribe in footer

Compliance

- CAN-SPAM, CASL, GDPR, UAE PDPL
- Unsubscribe honoured within 48 hours
- Privacy notice linked

MONITORING

The health dashboard, checked weekly

Green on every line equals perfect health. Any red pauses bulk sending that day.

METRIC	GREEN	AMBER	RED
DMARC aligned pass	99%+	95 to 99%	under 95%
Gmail spam rate	under 0.08%	0.08 to 0.1%	over 0.1%
Hard bounce rate	under 0.5%	0.5 to 2%	over 2%
Unsubscribe rate (bulk)	under 0.3%	0.3 to 0.8%	over 0.8%
Blocklist listings	0	minor list	Spamhaus or major
Seed inbox placement	90%+	80 to 90%	under 80%
TLS-RPT failures	0	1 to 5	over 5
mail-tester score	10	9 to 9.9	under 9

RECOMMENDED TOOLKIT

The tools that run the Email Outreach Engine

The chosen toolkit carries through every document, platform and checklist step.

Apollo

Lead generation

Find ICP contacts and enrich them through the Claude connector

Claude + Apify

Research and scrapers

Buying signals, lead scoring, personal lines and copy

MillionVerifier

Recipient verification

Bulk check every lead before it enters a campaign

NeverBounce

Recipient verification

Second check on catch-all and unknown results

Mailscale

Inboxes and test runs

Native inboxes on the sending domains, marketing-style test runs

PlusVibe

Sending engine

Warmup, inbox rotation, spintax, campaigns, replies, casual inbox tests

mail-tester

Deliverability score

10/10 check for the main domain and every sending inbox

Claude

AI and automation layer

Skills, health reports, evidence checks, meeting briefs and scopes

SERVICE PROVIDERS

Suggested vendors for every part of the engine

Your chosen tools stay first; alternatives and indicative 2026 prices. Confirm current prices before buying.

Need	Suggested	Alternatives	Indicative price
Sending domains	**Cloudflare Registrar**	Porkbun, Namecheap	About $10 to $12 a year per .com at cost
Cold inboxes (Microsoft and Google)	**Mailscale (chosen)**	Maildoso, Zapmail, InboxKit, Primeforge	Quote per inbox; market range about $2.50 to $4.50 per Microsoft inbox a month
Sending, warmup and unibox	**PlusVibe (chosen)**	Instantly, Smartlead	From about $37 a month; warmup included
Lead data	**Apollo (chosen)**	Clay, Lusha	Paid seat plans; check current Apollo pricing
Research and scraping	**Claude + Apify (chosen)**	PhantomBuster	Apify usage-based, free tier then paid plans
Email verification	**MillionVerifier (chosen)**	ZeroBounce, Bouncer	About $37 per 10,000 checks
Second verification pass	**NeverBounce (chosen)**	Scrubby for catch-all domains	About $80 per 10,000 checks
DMARC monitoring	**EasyDMARC**	dmarcian, DMARCLY, Postmark DMARC digests (free)	Free tier; paid from about $18 to $36 a month for 2 domains
Deliverability score and placement	**mail-tester, PlusVibe and Mailscale tests (chosen)**	GlockApps	mail-tester low-cost credits; GlockApps free 3 tests then from $59 a month
Reputation dashboards	**Google Postmaster Tools**	Microsoft SNDS	Free
Opt-in bulk email lane	**Brevo**	Amazon SES, Mailchimp	Brevo tiered plans; SES about $0.10 per 1,000 emails
CRM and pipeline	**HubSpot Starter**	Pipedrive	Per-seat monthly plans
Automation	**n8n**	Make, Zapier	Self-host free or cloud plans
Meeting booking	**Calendly**	Cal.com	Free tier; paid per seat
Team alerts	**Slack**	Microsoft Teams	Existing workspace

OWNERSHIP

Who does what

Clear owners keep the program on schedule.

Management

Approves policy moves (reject, bulk launch), signs off tenant changes

Microsoft 365 admin

DKIM, outbound spam policy, MFA, SMTP AUTH, Defender reviews

Cloudflare / DNS owner

All records, DNSSEC, MTA-STS hosting, web proxy consistency

Marketing ops

Bulk platform, lists, consent, content, ramp schedule

Deliverability analyst

Weekly dashboard, DMARC and TLS reports, blocklist watch

Claude (this project)

Weekly DNS and blocklist sweep, report summaries, record generation, header analysis

NEXT 72 HOURS

Ability

Eight actions to move from 4/10 toward 10/10

1. **Enable DKIM and publish both CNAMEs in Cloudflare**
2. **Change DMARC rua to a DMARC monitor**
3. **Freeze any bulk or mass mail from abilityglobal.io**
4. Send header tests to Gmail and Outlook.com
5. Verify the domain in Google Postmaster Tools
6. Run MXToolbox Domain Health, Blacklist and Spamhaus
7. List every system that sends as the domain
8. Confirm full admin control of the Microsoft 365 tenant

DKIM live: 17 Sep | DMARC reject: by 31 Oct | Perfect health and bulk lane ready: 1 Nov 2026