FICTIONAL MSP PORTFOLIO REPORT

DMARC operations decision report

Prepared for Northstar Managed Services using reserved **example.*** domains and synthetic data. This document demonstrates a reporting method; it does not represent a customer, production domain, security outcome, or deliverability result.

Report period: 11-17 August 2026 UTC Revision: 2.0 Last reviewed: 18 August 2026

> **Decision boundary: aggregate evidence supports investigation and policy review. Production DNS or policy changes require separate owner confirmation, approval, validation, and rollback planning.**

Executive decision summary

Domains	Represented messages	DMARC aligned	Observed sources	Unresolved sources	Open decisions
3	9,100	8,540 (93.8%)	7	1	3

Portfolio review states

Domain	State	Reason	Decision needed
client-a.example	Ready for policy review	Material sources confirmed; one aligned vendor path validated; rollback criteria recorded.	Approve a controlled policy change or continue observation.
client-b.example	Blocked	One material CRM source remains unresolved and SPF is not aligned.	Confirm owner and expected sending identity.
client-c.example	Continue observation	Only two participating receivers are represented in the current period.	Collect broader receiver evidence before review.

Decisions completed

- Client A confirmed **Example CRM** as an authorized sender and assigned Marketing Operations as owner.
- Client A validated an aligned DKIM signature for the synthetic CRM stream.
- Client C documented its current receiver-coverage limitation and next review trigger.

Decisions requiring approval

- Client A: approve or defer the proposed controlled policy change.
- Client B: confirm whether the unresolved CRM source is authorized, obsolete, or unauthorized.
- Client C: approve continued observation until broader report evidence is available.

Next review: 25 August 2026

DOMAIN EVIDENCE

Reported evidence by domain

Mechanism authentication and DMARC identifier alignment are different tests. The aligned columns below describe DMARC alignment, not raw SPF or DKIM authentication alone.

Domain	Report period UTC	Published policy	Represented messages	SPF aligned	DKIM aligned	DMARC aligned
client-a.example	11-17 Aug	p=none	5,200	3,900	4,980	5,030
client-b.example	11-17 Aug	p=none	2,870	1,940	2,300	2,480
client-c.example	11-17 Aug	p=quarantine	1,030	1,010	1,030	1,030

Domain	Unresolved sources	Open decisions	Review state	State reason
client-a.example	0	1	Ready for policy review	Relevant sources confirmed; material alignment issue closed; named approver and rollback criteria recorded.
client-b.example	1	1	Blocked	Material source ownership and expected identity remain unresolved.
client-c.example	0	1	Continue observation	Current report set has limited receiver coverage.

Evidence notes

- **SPF aligned** and **DKIM aligned** identify messages whose authenticated mechanism also aligned with the Author Domain.
- **DMARC aligned** counts represented messages with at least one aligned authenticated identifier; it is not the sum of the SPF and DKIM columns.
- A reported disposition records receiver policy evaluation. It is not proof of final inbox placement.
- Source counts group observed technical sources. They do not automatically equal business systems or threat actors.

Synthetic source example

Observed evidence	Inference	Client confirmation	Approved action
192.0.2.44; 420 messages; DKIM aligned; SPF not aligned	Likely Example CRM; medium confidence	Marketing Operations confirms authorized use	Validate aligned DKIM, then include in policy-review record

OWNED ACTION REGISTER

Evidence, ownership, and approval

An unfamiliar source remains unresolved until evidence and an authorized business owner establish its status. Unknown does not mean malicious.

A-01 - Client A CRM alignment

Observed evidence	192.0.2.44; 420 represented messages; SPF authenticated but not aligned; DKIM authenticated and aligned.
Likely service / confidence	Example CRM / medium, based on return path and selector pattern.
Client-confirmed owner	Marketing Operations.
Authorization state	Authorized.
Proposed action	Keep the aligned DKIM path documented and validate it through the next report set.
Action owner / approver	MSP email engineer / Client IT owner.
Validation / rollback	Confirm continued aligned DKIM evidence; no DNS change is proposed in this action.
Status / next review	Validated / 25 August 2026.

A-02 - Client B unresolved CRM source

Observed evidence	198.51.100.28; 260 represented messages; SPF authenticated but not aligned; no aligned DKIM signature.
Likely service / confidence	Possible sales platform / low; evidence is incomplete.
Client-confirmed owner	Unconfirmed.
Authorization state	Unresolved.
Proposed action	Ask application owners to confirm the service, business purpose, and intended From identity.
Action owner / approver	MSP service manager / Client IT owner.
Validation / rollback	Require owner confirmation and new aligned evidence before any policy proposal; no blocking action.
Status / next review	Blocked / 21 August 2026.

A-03 - Client C evidence coverage

Observed evidence	1,030 represented messages from two participating receivers; all represented messages DMARC aligned.
Likely service / confidence	Known Microsoft 365 sending paths / high, based on client inventory.
Client-confirmed owner	Client IT.
Authorization state	Authorized within the represented data.
Proposed action	Continue observation until the stated receiver-coverage condition is met.
Action owner / approver	MSP email engineer / Client IT owner.
Validation / rollback	Add the next report period and compare receiver participation; current policy stays unchanged.
Status / next review	Continue observation / 25 August 2026.

METHOD AND LIMITATIONS

How this fictional report was prepared

Included evidence

- Synthetic RFC 9990 aggregate records for 11-17 August 2026 UTC.
- Records deduplicated using reporting organization plus report ID.
- Message totals calculated by summing included aggregate-record counts.
- DMARC-aligned counts include messages with at least one aligned authenticated SPF or DKIM identifier.
- Ownership states require an explicit client or MSP confirmation record; technical clues remain labelled as inference.

Policy-review workflow

1. Confirm report coverage and the current published policy.
2. Inventory observed sources and identifiers.
3. Separate authentication from alignment results.
4. Confirm ownership and authorization state.
5. Close or explicitly accept material exceptions.
6. Prepare the proposed policy decision, validation, and rollback plan.
7. Obtain approval from the authorized MSP or client decision-maker.
8. Execute through the approved production-change process.
9. Validate new evidence and record the result.

The historic **pct** tag is not used in this recommended workflow, and no fixed clean-day threshold authorizes a policy transition.

Limitations

This fictional report summarizes only the aggregate-report files included for the stated period. It may not represent all receivers or all mail using the example domains. Aggregate evidence does not by itself prove business ownership, authorization, malicious intent, delivery outcome, or policy safety. All production changes require separate approval and validation.

- A source IP can represent infrastructure shared by multiple systems.
- A message can carry multiple DKIM signatures and authentication results.
- A DMARC pass does not prove that a sender is authorized for a business purpose.
- Receiver participation and reporting completeness vary.
- Failure reports can contain non-public information and need separate privacy controls.

Current standards

RFC 9989: DMARC
RFC 9990: DMARC Aggregate Reporting
RFC 9991: DMARC Failure Reporting

Prepared by MailAuthOps. Public operator: Preksha Shukla. Technical-evidence reviewer: Devam Parikh. Revision 2.0.