RDA DELIVERABILITY

SAMPLE DELIVERABLE

Law Firm Communication Trust Health Check

Email authentication, sender alignment and domain protection

Northbridge Legal Group

northbridgelegal.example

REPORT TYPE	ASSESSMENT DATE	OVERALL POSITION
Illustrative sample	08 July 2026	**Needs attention**

Fictional environment. No live client systems or confidential data were assessed.

DECISION BRIEF

What the evidence says

OVERALL POSITION	HIGH PRIORITY	MEDIUM PRIORITY	HEALTHY
Needs attention	3 findings	2 findings	3 controls

PLAIN-ENGLISH CONCLUSION

Microsoft 365 authentication is in good shape, but not every system sending as @northbridgelegal.example is aligned consistently. The website form and CRM path should be corrected and verified before DMARC is moved beyond monitoring.

The three actions that matter first

01 **Correct the website sender path**

Use a controlled business-domain From address and place the visitor address in Reply-To.

02 **Complete CRM authentication**

Enable and verify custom-domain DKIM and confirm DMARC alignment.

03 **Validate before enforcing**

Progress DMARC only after legitimate senders are known, passing and documented.

Assessment principle
This sample separates verified controls from unresolved risk. A live RDA assessment uses public DNS, onboarding evidence, sender inventory and validation results - not a single automated scan.

ENVIRONMENT

What was reviewed

The assessment maps who sends for the primary domain, how those systems authenticate and whether the identities align.

PRIMARY DOMAIN	BUSINESS TYPE	EMAIL PLATFORM
northbridgelegal.example	Fictional US law firm	Microsoft 365
KNOWN SENDERS	**POLICY POSITION**	**CLASSIFICATION**
M365, web form, CRM	DMARC monitoring (p=none)	Illustrative sample

Assessment coverage

DNS & POLICY	SPF, DMARC, relevant DKIM evidence, alignment indicators and visible authorization paths.
SENDING SOURCES	Known business platforms and evidence of services that may send using the domain.
OPERATIONAL CONTEXT	Expected mail flow based on onboarding answers and supporting evidence.
RISK & PRIORITY	Whether a condition is healthy, needs validation or should be corrected before policy progression.

SCOPE BOUNDARY
This report focuses on email authentication and domain trust. It does not guarantee inbox placement, prevent every form of fraud, or replace endpoint security, identity security or user-awareness controls.

RISK REGISTER

Findings at a glance

ID	FINDING	PRIORITY	ASSESSMENT
F-01	DMARC remains in monitoring mode	**HIGH**	Policy is published as p=none.
F-02	Website form sender is not consistently aligned	**HIGH**	Form mail can use an address path that fails DMARC alignment.
F-03	CRM platform DKIM is incomplete	**HIGH**	Aligned DKIM should be verified before enforcement.
F-04	SPF authorization is valid but brittle	**MEDIUM**	Record is near the practical lookup ceiling and includes legacy scope.
F-05	Legacy sender authorization needs confirmation	**MEDIUM**	An older service appears to remain permitted to send.
H-01	Microsoft 365 DKIM verified	**HEALTHY**	Primary mail signs with an aligned domain.
H-02	SPF syntax currently valid	**HEALTHY**	Published SPF record is syntactically valid.
H-03	DMARC reporting is enabled	**HEALTHY**	Aggregate reporting is configured for visibility.

PRIORITY LOGIC HIGH - correct or fully investigate before enforcement. MEDIUM - improve after critical alignment issues are controlled. HEALTHY - verified in the reviewed evidence; continue monitoring.

HIGH PRIORITY

Authentication and policy

01 DMARC remains in monitoring mode

HIGH

FINDING	A DMARC record is published, but the requested receiver policy is p=none. The domain is collecting information rather than requesting quarantine or rejection for failed mail.
EVIDENCE REVIEWED	`v=DMARC1; p=none; rua=mailto:dmarc@...`
WHY IT MATTERS	Monitoring is a useful starting point, but it does not create an enforcement position. Moving too early can disrupt legitimate senders.
RECOMMENDED NEXT ACTION	**Confirm all legitimate sending sources, correct alignment gaps, review reporting evidence and then progress policy in controlled stages.**

02 Website form sender is not consistently aligned

HIGH

FINDING	The website form can submit mail using an address path that is not consistently authenticated and aligned with the business domain.
EVIDENCE REVIEWED	Test messages and configuration evidence show the form can place a visitor address in the visible From field while relaying through the website host.
WHY IT MATTERS	The authenticated domain can differ from the visible From domain, causing DMARC failure and avoidable reply-handling problems.
RECOMMENDED NEXT ACTION	**Send from a controlled address on the business domain using an authenticated relay. Put the visitor address in Reply-To, then retest SPF, DKIM and DMARC alignment.**

HIGH PRIORITY

Third-party sender alignment

03 CRM platform DKIM is incomplete

HIGH

FINDING	The CRM / marketing platform is a legitimate sender, but aligned DKIM has not yet been fully verified for mail using the business domain.
EVIDENCE REVIEWED	Platform configuration and message evidence indicate mail can be sent for the domain without a consistently aligned DKIM signature.
WHY IT MATTERS	A legitimate sender that is not aligned can become collateral damage when DMARC enforcement is strengthened.
RECOMMENDED NEXT ACTION	**Enable the platform's custom-domain DKIM, publish the required DNS records, validate signing and alignment, then confirm DMARC pass before policy progression.**

How the issues connect

1 **MONITORING POLICY** — DMARC is not asking receivers to enforce a failure outcome.

2 **ALIGNMENT GAPS** — The website form and CRM are not yet consistently aligned.

3 **ENFORCEMENT DEPENDENCY** — Correct legitimate senders before strengthening policy.

DO NOT JUMP DIRECTLY TO p=reject

Legitimate senders still have unresolved alignment gaps. Correct the sending paths first, validate the result and then progress policy deliberately.

SECONDARY CONTROLS

Authorization and maintenance

04 SPF authorization is valid but brittle

MEDIUM

FINDING	The SPF record is syntactically valid, but its authorization chain is close to the practical DNS-lookup limit and includes a service that may no longer be required.
EVIDENCE REVIEWED	`v=spf1 include:spf.protection.outlook.com include:crm.example include:legacy.example -all`
WHY IT MATTERS	SPF is easier to break when services are added without reviewing the full chain. Legacy includes can leave unnecessary authorization in place.
RECOMMENDED NEXT ACTION	**Confirm the legacy service, remove it if unused, document the sender inventory and re-check lookup count after every sender change.**

05 Legacy sender authorization needs confirmation

MEDIUM

FINDING	An older service appears to remain authorized through the SPF chain, but it is not listed as a current business sender.
EVIDENCE REVIEWED	The include remains visible in the published SPF path while onboarding evidence lists Microsoft 365, the website form and the current CRM platform.
WHY IT MATTERS	Unnecessary sender authorization expands the environment that must be understood and maintained.
RECOMMENDED NEXT ACTION	**Confirm ownership and current use. Remove authorization only after the business confirms the service is no longer required.**

HEALTHY CONTROLS

What is working

H-01

Microsoft 365 DKIM

Aligned signing verified for the primary business email platform.

H-02

SPF syntax

Published record is syntactically valid at the time of assessment.

H-03

DMARC reporting

Aggregate reporting is configured, providing a basis for sender validation.

Ongoing assurance point

New vendors, subdomains, staff tools, website changes and DNS edits can alter the authentication environment over time. Periodic verification catches drift before it becomes a communication-risk issue.

Verified today | Documented for handoff | Re-check after material sender or DNS changes

CONTROLLED CHANGE

Recommended order of work

The sequence is designed to strengthen the environment without interrupting legitimate mail.

01

CONFIRM SENDER INVENTORY

Validate M365, website form, CRM and the legacy SPF include.

EVIDENCE OF COMPLETION

Approved sender list

02

CORRECT ALIGNMENT GAPS

Reconfigure the website form and enable aligned CRM DKIM.

EVIDENCE OF COMPLETION

Test messages pass DMARC

03

CLEAN AUTHORIZATION

Remove confirmed legacy scope and re-check SPF behavior.

EVIDENCE OF COMPLETION

Simplified SPF path

04

VALIDATE BEFORE ENFORCEMENT

Review reporting evidence, exceptions and unexpected sources.

EVIDENCE OF COMPLETION

Stable pass pattern

05

PROGRESS POLICY SAFELY

Move from monitoring to staged enforcement only when ready.

EVIDENCE OF COMPLETION

Controlled change + verification

CONTROL POINT: A stronger DMARC policy is useful only after legitimate senders are accounted for and aligned. A public p=none result alone is not a sufficient reason to enforce.

HANDOFF

What the client leaves with

01	**Clear understanding**	What is healthy, uncertain and in need of attention.
02	**Prioritised findings**	A documented list separated by urgency and business impact.
03	**Technical evidence**	The records, alignment observations and sender evidence behind each conclusion.
04	**Remediation roadmap**	A controlled order of work designed to avoid blind DNS or policy changes.
05	**Decision point**	A clear basis for deciding what work should be scoped next.

WHAT HAPPENS NEXT IN A REAL ENGAGEMENT

RDA reviews the findings with the client. If remediation is justified, the work is scoped separately according to the actual environment, ownership boundaries and systems involved. No change is recommended solely because an automated scan produced a warning.

HEALTH CHECK → UNDERSTAND → REMEDIATE → VERIFY

Sample report note
Northbridge Legal Group and northbridgelegal.example are fictional. Findings, records and evidence are illustrative and contain no live-client or confidential data.

RDA Deliverability

rdadeliverability.com