

File-Exchange Exposure Map

Date: _____
Firm: _____

A working artifact from your 30-minute diagnostic session

1 Exposure Surface

Four diagnostic questions. Answer each in your own words during the briefing.

01 External parties currently exchanging regulated data via our MFT (rough count, with breakdown by data sensitivity: PHI / PCI / financial / contractual)

02 Credentialing model and rotation cadence (individual, shared, or service-bound; rotation frequency)

03 Last audit or examiner evidence request (what we produced, how long it took, what wasn't covered)

04 Breach-notification readiness if our MFT vendor were compromised (obligation timeline, capability gap, current containment posture)

2 Buyer Scorecard

My evaluation criteria, independent of my team's technical criteria

The four answers below become the framework I take to my security committee or board.

01 What my board needs to hear about file-exchange risk this cycle:

02 The audit finding or examiner question that would force urgency:

03 My biggest current evidence gap:

04 What "good" looks like for me, vendor-agnostic:

3 Path

Three paths CISOs in this position typically take. Mark the one your organization is closest to today.

☐ Status Quo + Hardening

Keep incumbent; invest in tighter rotation, audit prep tooling, supplemental monitoring.

☐ Renewal with Stricter Reqs

Use next renewal as leverage for evidence-pack, breach response, credential model improvements.

☐ Platform Replacement

Scope a 12–18 month replacement program addressing architectural root cause.

My org is closest to:

My board would support:

The gap between those is: