

Can your firm prove how client PDFs were handled?

Mark Yes only when the control is consistent and you could produce evidence. Count each Yes, then use the score on page 2.

FIRM / TEAM: _____

DATE: _____

- | | | |
|-----------|---|--|
| 1 | Approved intake
Do client PDFs arrive through a documented, access-controlled channel rather than personal email or ad hoc links? | YES ☐ NO ☐ |
| 2 | Minimum access
Can you show that only assigned team members can access each client PDF? | YES ☐ NO ☐ |
| 3 | Approved tools
Are staff required to use approved PDF tools with known processing and retention behavior? | YES ☐ NO ☐ |
| 4 | Local or disclosed processing
Can you state where PDF bytes are processed and which providers can receive them? | YES ☐ NO ☐ |
| 5 | Sensitive-data check
Is there a repeatable check for PII, hidden content, comments, and metadata before delivery? | YES ☐ NO ☐ |
| 6 | Output verification
Does someone verify the exported PDF for completeness, readability, and unintended disclosure? | YES ☐ NO ☐ |
| 7 | Secure delivery
Are deliverables shared through a controlled channel with recipient and expiry safeguards? | YES ☐ NO ☐ |
| 8 | Retention rule
Does every client PDF have a documented retention and deletion rule tied to the engagement? | YES ☐ NO ☐ |
| 9 | Handling evidence
Can you produce a metadata-only record of the tool, time, outcome, and handling method? | YES ☐ NO ☐ |
| 10 | Incident readiness
Can your team quickly identify affected work, owners, and evidence if a handling concern arises? | YES ☐ NO ☐ |

Score your handling posture

TOTAL YES ANSWERS: / 10

0-3 | HIGH RISK

Handling is difficult to defend. Prioritize approved tools, access rules, retention ownership, and a basic evidence trail.

4-7 | DEVELOPING

Some controls exist, but inconsistency creates exposure. Document the weak stages and assign owners and evidence requirements.

8-10 | STRONGER

Your foundation is stronger. Test whether the evidence is complete, client-safe, and consistently produced across teams.

Recommended minimum controls

- Publish one approved intake-to-deletion workflow and name an owner.
- Use least-privilege access and remove access when the engagement ends.
- Prefer browser-local processing; document every provider that receives PDF bytes.
- Require sensitive-data preflight and final-output verification before delivery.
- Set retention by engagement and record deletion or non-retention consistently.
- Create client-safe proof containing workflow metadata, never document content or filenames.

SEE WHAT CLIENT-SAFE PROOF LOOKS LIKE

Open an illustrative deletion receipt

[Learn about Vault PDF browser-local processing and receipts](#)

Educational use only. This checklist is general information, not legal, regulatory, insurance, or information-security advice. It does not determine compliance. Consult qualified advisers and your client requirements.