The system nobody bought

Free web converters are the least-governed software in most professional firms — and the only one that touches every client file

For managing partners, IT and compliance leads at accounting, audit and law firms of 10 to 100 people | 25 August 2026

Your firm has a document management system it paid for, a backup policy it reviews, and an IT provider it can name. It also has a second document system that appears on no invoice, in no policy and on no asset register: whichever free conversion website a junior found the last time a file would not upload.

That system handles the same client files as the one you bought. This paper is about why it exists, what actually happens to a file once it is uploaded, and a five-point audit a partner can run this week without buying anything.

1. The system nobody bought

Ask a partner which systems hold client data and you will get a confident list: the practice management suite, the document store, the email tenant, the portal. Every one of them was procured, has an owner, and appears in the firm's own risk register.

Now ask what happens when a 60 MB scanned balance sheet will not go through a 20 MB portal limit at half past six. The answer is not on the list, has no owner, and was chosen in about forty seconds by whoever was holding the file.

This is not a hypothetical failure. It is the ordinary way work gets done under a deadline, and it is invisible precisely because it works — the file gets smaller, the deadline is met, and nothing anywhere records that a client's audited accounts spent four minutes on a server in a country nobody identified.

> *The distinguishing feature of this system is not that it is insecure. It is that it is ungoverned: no contract, no owner, no log, and no way to answer a client who asks where their file has been.*

2. Why capable people do this

It is tempting to treat this as a training problem. It is not. Three structural decisions make it the rational choice for the person doing the work.

The licence economics

A full editing suite costs enough per seat that most firms buy it for the people who need it daily — a partner, a manager, whoever produces the final PDF. The junior scanning, splitting and compressing forty files a week is precisely the person who is not given a licence, and precisely the person handling the most raw client material.

The size limit with no exit

Firms set upload limits and then provide no compliant way to meet them. A 20 MB cap with no supported way to get a 60 MB scan under it is not a control; it is an instruction to find one.

The deadline

Nobody evaluates a vendor at 18:30 on a filing deadline. They search, they click the first result, they get the file back, and they move on. Any policy that depends on somebody doing otherwise, under that pressure, with no alternative to hand, is a policy that describes an intention rather than a practice.

> *The control failure is upstream of the person who clicked. The firm created the constraint, declined to provide a compliant way to meet it, and left the tooling decision to whoever was under the most time pressure.*

3. What "secure cloud processing" actually means

Free conversion services are not usually careless, and most describe their security accurately. The problem is what that description covers.

Encryption in transit is not the question

A padlock in the address bar means the file was encrypted between the browser and the server. That is worth having, and it is not the risk. To compress, convert or redact a document, a server has to **decrypt it and hold the plaintext in memory and usually on disk**. For that interval, the client's document exists in readable form on a machine your firm has never assessed, operated by a company it has no contract with.

"Files deleted after one hour" is a retention policy, not a security control. It describes when a copy stops existing, not who could read it while it did, where it was replicated, or what the backups do.

Read the terms, not the marketing

Rather than take anyone's characterisation of these services — including this one — the useful exercise is to open the terms of service of whichever tool your staff actually use and look for two things: the licence you grant over uploaded content, and the stated purposes for which files may be processed or retained. Terms vary widely, and some are perfectly reasonable. The point is that **your firm has accepted them on a client's behalf without reading them**.

That is the part a client would find hard to accept, and it holds regardless of how any particular provider behaves.

> *There is a second question worth asking of any hosted tool: could the provider comply with a lawful demand from its own jurisdiction for a document you hold under professional privilege? Usually the answer is yes, and it will not involve you.*

4. Where this lands professionally

Two obligations bite here, and they bite independently of each other.

Confidentiality is a professional duty before it is a statutory one. An engagement letter, and the codes of conduct behind it, commit the firm to controlling client information. Disclosure to an unassessed third party is a breach whether or not any personal data was involved and whether or not anything went wrong.

The DPDP Act, 2023 adds a statutory layer where the documents contain personal data, which for KYC packs, payroll and most client files they do. A firm determining how that data is processed carries the obligations of a Data Fiduciary, including reasonable security safeguards, with penalties reaching Rs 250 crore for failing to take them.

> *This paper describes what software does and is not legal advice. No provision cited here has been reviewed by a practitioner on the authors' behalf; your own adviser should map any obligation to your circumstances. The regulatory analysis is covered at greater length in our paper on endpoint compliance for digital lenders.*

The uncomfortable part for a partner is evidential rather than legal. If a client asks where their file has been, a firm using an unlogged web tool cannot answer. There is no record to produce, because the system that handled the document was never a system anyone was managing.

5. The triage desk

The fix is not to buy every member of staff a full editing suite. Most of what juniors do to documents is triage — make it smaller, open it, take pages out, take names out, put it together, send it on — and triage does not need an editor. It needs to happen somewhere governed.

Oxofolio is a desktop application for that work. It opens no network sockets, so a document processed in it has not been anywhere. What that means in practice:

THE DAILY JOB	WHAT HAPPENS INSTEAD
The 60 MB scan that will not upload	Re-encoded locally, with the real saving shown per file before anything is kept. A page carrying real text is never flattened to hit a size target.
Forty protected bank statements	Opened in one pass with passwords the firm already holds. No password is written to disk or recorded in any log.
Aadhaar and PAN in a KYC bundle	Found by checksum rather than pattern, shown in place, removed from the file itself, and the output re-read to confirm they are gone.
A scan nobody can search	OCR runs from an engine bundled in the installer, so it works with the network unplugged.
“Where has this file been?”	A processing log records every operation, when, on which machine, with the SHA-256 of every input and output.

That last row is what converts this from a security purchase into a defensible one. The firm stops relying on the absence of an incident and starts holding a contemporaneous record of what was done to which file.

What it does not do

- **It does not edit Office files.** The spreadsheet, document and presentation viewers read and never write. This is a triage desk, not a replacement for Word or Excel.
- **It does not recover passwords.** It applies keys the firm already holds — no brute force, no dictionary. A tool that cracked passwords would be a liability on a firm's asset register.
- **It does not make the firm compliant.** It produces evidence and does work that would otherwise be done by hand. Compliance remains a property of the firm's processes.

It can also hand a document to Excel or Numbers when real editing is needed. That opens no socket, but it is worth stating plainly: **Numbers saves into iCloud Drive by default, and Excel signed into a Microsoft account turns AutoSave on and places the file in OneDrive.** The application says so at the point of the click. For a firm, this is a policy question — the same configuration governing those services for every other document governs it here.

6. A five-point audit you can run this week

None of this requires a purchase, and all of it produces an answer a partner can act on.

- **1. Ask, do not survey.** Ask three juniors what they do when a file is too large to upload. Ask as a process question, not a compliance one — you want the real answer, and a survey with the firm's name on it will not get it.
- **2. Look at the outbound logs.** Whoever runs your firewall or DNS can tell you in an afternoon which document-conversion domains were reached in the last ninety days, and how often. Volume matters more than the list: this is usually routine rather than occasional.
- **3. Open a file you sent last week.** Take a PDF that went to a client and check its properties for author, producing software and previous titles. Then take a spreadsheet and look for hidden rows and the workings behind a summary. Documents routinely carry more than they display.
- **4. Test one redaction.** Take a document where an identifier was blacked out, open it in any reader, and try to select the text under the mark. If it selects, every document redacted that way is still carrying what it was supposed to have lost.
- **5. Find the size limit with no exit.** List every upload cap staff meet — portal, email, regulator — and for each one write down the supported way to comply. Any blank is a place the firm is relying on somebody improvising.

> *Points 3 and 4 tend to be the ones that change a partner's mind, because they are checks on work the firm has already delivered rather than predictions about what might happen.*

7. Conclusion

The exposure in a professional services firm is rarely the system that was bought and reviewed. It is the one that was never chosen at all — adopted quietly, by capable people, because the firm set a constraint and did not provide a way to meet it.

Closing it does not require a new policy. It requires the compliant path to also be the fastest one, so that at half past six on a deadline the tool already on the desktop is the obvious thing to reach for. Until that is true, no amount of policy will beat a search engine.