Agent Access Review: Marlowe & Datta Tax Advisors

Sample report. Marlowe & Datta is a fictional 12-person tax and accounting practice. This shows the format and depth of a real report. No real firm is described.

Review date: [date] · Reviewed by: Stephen Pritchett, Gatepost Review · Report for: the managing partner

Summary. We found 7 AI tools and automations across the firm's email, document storage, practice software and client portal, and 7 findings: 2 High, 2 Medium, 2 Low and 1 set up well.

Fix first: delete the former contractor's access key to the practice software. It takes about five minutes and closes the most serious gap.

Scope and limits

- **Reviewed:** the firm's email accounts and their connected apps, the shared document drive, the practice management software, the tax research subscription, the client portal and the automation tool, as listed in the signed agreement.
- **Access used:** read-only, plus a screen share with the managing partner for two settings pages. No setting was changed.
- **Date:** settings as they stood on [date]. They can change after it.
- **Not covered:** attack testing, the accuracy of any tool's output, staff laptops, and the items listed under "Not reviewed". This is an access review, not a guarantee of security and not legal advice.

Agent inventory

Tool	What it does	Owner	Connected to	Can change or send?	Approval ?	Log?
Email drafting assistant	Drafts and sends client replies	Partner A	Partner A's mailbox: read, send, delete	Yes: sends as the partner	No	No
Former contractor's access key	Built for a 2025 software migration	None (contractor left)	Practice software: full admin	Yes: everything	No	No
Tax research assistant	Answers research questions from firm files	Senior manager	Every client folder: read and write	Yes: can edit files	No	Partial
Document intake bot	Sorts client uploads into folders	Office manager	Client portal uploads: read only	No	Not needed	Yes
Meeting notes tool	Records and summarises client calls	Partner B	Calendar, video calls, notes drive	No	Not needed	Yes
Invoice reminder workflow	Emails clients about unpaid invoices	Bookkeeper	Practice software (billing), firm mailbox	Yes: sends email	No	Yes
Browser AI extension	Summarises web pages and documents	Unknown; staff installed it	Whatever is open in the browser	No	Not needed	No

Findings and fixes

#	Rating	Tool	What we found	Why it matters	Fix
1	High	Former contractor's access key	A key with full admin rights to the practice software, created for a contractor who left in the spring, has no owner and no log.	Anyone holding a copy can read every client's return, change records or export the client list, and nobody would see it.	Delete the key today. Then check the software's activity history for its use since the contractor left.
2	High	Email drafting assistant	Can send and delete mail as Partner A with no review and no log.	A wrong reply goes out in the partner's name to a client or the IRS, and a deleted message cannot be traced.	Switch it to drafts only and remove its delete permission. Partner A sends.
3	Medium	Tax research assistant	Has read and write access to every client folder. Its job only needs reading.	A tool error or a breach at the vendor could alter or remove client records across the whole firm.	Reconnect it with read-only access, limited to the research folder if the vendor allows it.
4	Medium	Browser AI extension	Installed by three staff on their own. It can read any page open in the browser, including the client portal and webmail. No one owns it.	Client data in open tabs can leave the firm with no record, and the vendor's terms were never reviewed.	Decide whether to allow it. If yes, name an owner and review the vendor's data terms. If no, remove it and add it to the AI policy.
5	Low	Invoice reminder workflow	Sends from the shared firm mailbox with no approval step and no cap on how many reminders it can send.	A bug could email every client at once, or send reminders to clients who have paid.	Add a daily send limit and route the first reminder of each run to the bookkeeper for a quick check.
6	Low	Whole firm	No written list of AI tools, who owns each, or what it can reach. The written information security plan does not mention them.	New tools get added and forgotten, which is how finding 1 happened. The FTC Safeguards Rule expects service providers to be overseen.	Keep this inventory as a living list, add it to the WISP, and review it each quarter.
7	Fine	Document intake bot	Read-only access to portal uploads, a named owner and a full log.	Nothing to fix.	Use it as the model for every new tool.

The meeting notes tool was also reviewed and is set up well: a named owner, no ability to change anything, and a log. One note for the partners: confirm clients are told that calls are recorded, which is a legal question outside this review.

Not reviewed

Item	Why not
Staff laptops and phones	Outside the agreed scope
The tax software vendor's own AI features	Settings are controlled by the vendor; needs their security documents, which the firm has requested
The payroll provider's connection	No access was granted; the office manager can share a screen in a follow-up

What happens next

- The fixes are Marlowe & Datta's to make, in any order, though finding 1 should come first.
- The one-page partner summary and the IT fix list are attached separately so each goes to the right person.
- Evidence screenshots held by Gatepost Review are deleted 90 days after this date, or sooner on request.
- A re-check after the fixes, and a quarterly re-check, are available at a fixed fee, only if the firm wants them.

Gatepost Review · Stephen@GatepostReview.com · gatepostreview.com