



STALWART GOVERNED

AI & Security Governance · vCISO



AI & Security Sprint

Riverbend Tax & Books

ENGAGEMENT ID
SG-RVB-2026-S1

IN ANSWER TO
SG-RVB-2026-A1

FIELDWORK
2026-09-03 to
2026-09-04

EDITION
Sprint record
verifiable source
document

STATUS
FINAL

SAMPLE

This is a sample. Riverbend Tax & Books is a fictional business. Every finding, figure and name in this document was invented to show what a real one looks like. A real client's document is produced by the same method, from evidence gathered at the client.



Pete Saar · AI & Security Governance · vCISO
pete@stalwartgoverned.com · stalwartgoverned.com
Stalwart Governed LLC

Contents

What this is	3
What we turned on	4
C-01 · Client work kept in the firm's own AI workspace	5
C-02 · Signed data-processing agreements with AI vendors	6
C-03 · Multi-factor sign-in on systems that hold client information	7
C-04 · Access removal when people leave	7
C-05 · Each AI feature in the tax software decided in writing	8
What we built	8
Client cover letters drafted from the firm's templates, in its own AI workspace	9
What is still open, and why	10
C-05 · Each AI feature in the tax software decided in writing, waiting until 2026-09-15	10
Not yet confirmed	11
Sign-off	11
Record	12

AI & Security Sprint

Riverbend Tax & Books

Engagement ID SG-RVB-2026-S1

In answer to	SG-RVB-2026-A1 · sha256 of that audit's source document, not of this document: 7c85a72dd35fd03be367f03d32ec4e360ffb0877d6ea2221e78edaef2367f2eb
Fieldwork	2026-09-03 to 2026-09-04
Edition	Sprint record — verifiable source document
Status	FINAL

This is a sample. Riverbend Tax & Books is a fictional business. Every finding, figure and name in this document was invented to show what a real one looks like. A real client's document is produced by the same method, from evidence gathered at the client.

What this is

This record covers the Sprint: the changes made after the audit, and a follow-up review to confirm them. It lists what that follow-up review found, control by control, against the audit. Each grade is printed with its two inputs beside it. D is how sensitive the data is, and E is how far outside the firm's control it went. The full scale is printed in the audit. A control marked "Configured" is one the follow-up review confirmed at the agreed end point. For data sent to AI tools, that means the data stays on the firm's own machines or in an AI workspace the firm owns, on terms that rule out training on what is typed. Anything short of that is marked. Each evidence line ends with its source file's fingerprint: the first 16 characters of the file's SHA-256, taken when the file was collected. The full SHA-256 is kept with the engagement record.

The firm's own systems remain the record of every setting named here. This document reports what was seen in them, and nothing more.

What we turned on

Control		Status
C-01	Client work kept in the firm's own AI workspace	CONFIGURED
C-02	Signed data-processing agreements with AI vendors	CONFIGURED
C-03	Multi-factor sign-in on systems that hold client information	CONFIGURED
C-04	Access removal when people leave	CONFIGURED
C-05	Each AI feature in the tax software decided in writing	DEFERRED



C-01 · Client work kept in the firm's own AI workspace

Before the Sprint: PENDING. After: CONFIGURED — confirmed by the follow-up review at the agreed end point.

At the audit: Critical (D4×E3). At the follow-up review: Medium (D4×E1). That is the agreed end point, and the lowest grade this kind of data can have. The data now stays on the firm's own machines or in an AI workspace the firm owns.

In answer to **F-01**, a finding of the audit: Client tax information pasted into a personal AI chat tool.

What the follow-up review found.

- **ADM** "the firm's own AI workspace is live on a business plan with learning from inputs switched off and deletion after 30 days; the preparer's cover letters are now drafted there" — *ai-workspace-settings.png, data controls · fingerprint 8639fe154521f358...*
- **DOC** "the AI use policy, revised 2026-09-02 with the managing partner, names the approved AI tools, bans pasting client information into any other tool, and adds a check before anything is pasted; all nine staff have acknowledged it in writing" — *ai-use-policy-v2.pdf, p. 1 · fingerprint f7d7afa8c0247acd...*

What was done about the exposure before the fix.

- 2026-08-24 — The preparer stopped pasting client figures into the free tool the day it was found, during fieldwork.
- 2026-08-27 — The free tool's saved chat history was deleted and the account closed.
- 2026-08-28 — Whether anyone had to be told was decided with the firm's counsel. The decision and its reasons are theirs and are not recorded here.

C-02 · Signed data-processing agreements with AI vendors

Before the Sprint: PENDING. After: CONFIGURED — confirmed by the follow-up review at the agreed end point.

At the audit: Critical (D4×E3). At the follow-up review: examined, and found in place and working.

In answer to **F-02**, a finding of the audit: An AI tool that can learn from what is typed, with no data-processing agreement in place.

What the follow-up review found.

- DOC "the firm's own AI workspace runs under a signed data-processing agreement with learning from inputs switched off, and the free chat tool's account is closed" — *workspace-dpa.pdf, §2 and §5 · fingerprint ed268649a44696ac...*
- DOC "the written information security program, revised as version 3.1 on 2026-09-04, lists both AI services the firm has approved among the service providers it oversees, each with its data-processing agreement" — *wisp-v3.1.pdf, §7 · fingerprint 845d9e7fa06ce7ec...*

C-03 · Multi-factor sign-in on systems that hold client information

Before the Sprint: PENDING. After: CONFIGURED — confirmed by the follow-up review at the agreed end point.

At the audit: High (D4×E2). At the follow-up review: examined, and found in place and working.

In answer to **F-03**, a finding of the audit: No second sign-in step on systems that hold client information.

What the follow-up review found.

- ADM "the document-exchange portal now requires a second factor for every user, and all nine have one set up" — *portal-security-export.csv, sign-in policy · fingerprint dc51do8e6f8f66af...*

C-04 · Access removal when people leave

Before the Sprint: PENDING. After: CONFIGURED — confirmed by the follow-up review at the agreed end point.

At the audit: High (D4×E2). At the follow-up review: examined, and found in place and working.

In answer to **F-04**, a finding of the audit: Access not removed when people leave.

What the follow-up review found.

- ADM "the departed seasonal preparer's tax-software account is disabled, and a leaver checklist now covers every system that holds client data" — *tax-users-export.csv, all rows · fingerprint 6141f091104c5bef...*

C-05 · Each AI feature in the tax software decided in writing

Before the Sprint: PENDING. After: DEFERRED — not finished yet, by the client's own decision. The section after the controls explains why, and what contains the risk until it is done.

At the audit: High (D4×E2). At the follow-up review: High (D4×E2).

In answer to **F-05**, a finding of the audit: AI features switched on inside the tax software, with training terms unclear.

What the follow-up review found.

- **ADM** "the tax software's AI assistant is switched off for client files as a stopgap; the vendor's terms still do not say whether the assistant learns from client data" — *tax-software-settings.png, AI assistant · fingerprint 68d0041fodb2bcd...*

What we built

After the work above, we built the first improvement. It was timed the same way before the change and after it. Both timings are printed as they were taken. Neither is multiplied out to a week or a year, or turned into money.

Client cover letters drafted from the firm's templates, in its own AI workspace

What it is. The firm's shared cover-letter templates now live in its own AI workspace, which runs under a signed data-processing agreement and does not learn from what is typed. A preparer picks the template, and the workspace fills in the client's details. Each draft names the template it used and the client record each figure came from. No letter goes out until the preparer has checked every figure against that record and read the letter through.

In use since 2026-09-02.

Who uses it. The preparers who write client cover letters. The managing partner owns the templates and approves any change to them.

What it saves. 25 minutes a letter before the change, 9 after.

The timings, as captured.

- **OBS** "before the change, a preparer drafting client cover letters by hand from the firm's shared templates was timed on three letters: 25 minutes a letter" — *timing-notes.md*, §1 · captured 2026-08-31 · fingerprint 1acf34dfoa4a2fo1...
- **OBS** "after the change, the same preparer drafted three client cover letters from the same templates in the firm's own AI workspace, each draft naming its template and client record, and checked and edited each before it went out: 9 minutes a letter" — *timing-notes.md*, §2 · captured 2026-09-04 · fingerprint 1acf34dfoa4a2fo1...

What is still open, and why

One item from the audit is not finished yet. It was left open on purpose, and this section explains it in plain words. It covers what the item is, why it is waiting, what contains the risk in the meantime, and what happens next.

C-05 · Each AI feature in the tax software decided in writing, waiting until 2026-09-15

What it is. Riverbend's tax software has a built-in AI assistant. When it is switched on, it can send parts of a client's file to the company that makes the software, and that company's terms do not yet say whether it uses that information to teach its AI.

Why it is waiting. Riverbend is partway through a signed contract with the software maker, and the terms in that contract can only be changed when it renews on 2026-09-15. Asking for new terms before then would mean paying to break the contract early, and waiting eleven days costs nothing once the risk is switched off.

What contains the risk until then. The assistant has been switched off for client files, so nothing from a client's file is being sent to the software maker while this waits. Staff lose a convenience, not a capability: everything the assistant helped with can still be done by hand, the way it was done before the recent update switched it on.

What happens next. At renewal, Riverbend will ask the software maker to promise in writing that client information is not used to train its AI and is deleted on request. If the maker agrees, the assistant goes back on under those terms. If it will not, the assistant stays off, and our next review under the Retainer will say so.

Decided by Riverbend's managing partner on 2026-09-04.

Some fixes cannot be finished in the same week as the rest. The risk is contained today, and each fix has a set date. Every record we issue will keep listing each open item until it is closed.

Not yet confirmed

Area	Status
AI note-takers on client calls	Not examined again at the follow-up review. The audit's entry stands unchanged. To check it: list the apps connected to the calendar and the meeting software, and see which of them join client calls.

Sign-off

Prepared by Peter Saar, CISSP #2450556.

AI & Security Governance · vCISO.

Issued by Stalwart Governed LLC.

This record states what the follow-up review observed during the window named above. It is not a certification. It claims no configuration the review did not show.

**STALWART GOVERNED**
AI & Security Governance · vCISO
Engagement SG-RVB-2026-S1

Signed: Peter Saar · Date of issue: 2026-09-05



Record

This is a sample, and you can check it the way a client would: drop this file on our Verify page, <https://stalwartgoverned.com/verify>, and it will show as a sample we published, unchanged. It will never show as an issued document. The fingerprint in the first row is of this sample's source document, the file the row names. It is not the fingerprint of this PDF. The PDF has its own, and both are registered. On a real engagement, the source document is delivered with the PDF, so either file can be checked on our Verify page. The remaining rows identify this document's version and date the reference pack it cited.

sha256 of riverbend-asbuilt.md	b181dca60115bec57b6ceb58075ceb2f32ee059df907bbc12c92ca10f5c6eb92
length	162 lines · 10776 bytes
copy	1 of 1
version	d40fd37c5203 · cd154950a3cb
reference pack	2026-08-21
to check it	certutil -hashfile "riverbend-asbuilt.md" SHA256 (Windows) · shasum -a 256 "riverbend-asbuilt.md" (macOS) · sha256sum "riverbend-asbuilt.md" (Linux)

How this report was made

The findings, grades and recommendations in this report were decided by the firm. Each finding rests on evidence the firm collected, each grade is computed by the firm's fixed method, and each figure is read directly from the evidence. We used AI as a drafting tool within fixed rules for what a sentence may and may not say. In signing the report, we take full editorial responsibility for it and adopt the words as our own.