



STALWART GOVERNED

AI & Security Governance · vCISO



AI & Security Retainer

Riverbend Tax & Books

ENGAGEMENT ID
SG-RVB-2026-R1

PRIOR PERIOD
SG-RVB-2026-A1

THIS PERIOD
SG-RVB-2026-A2

EDITION
Period 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 held	4
P-01 · An AI note-taker joining client calls	4
P-02 · Client tax information pasted into a personal AI chat tool	5
P-03 · An AI tool that can learn from what is typed, with no data-processing agreement in place	6
P-04 · No second sign-in step on systems that hold client information	6
P-05 · Access not removed when people leave	6
P-06 · AI features switched on inside the tax software, with training terms unclear	7
Coverage this period	7
The period's work	9
Visits and calls	9
Maintenance	9
What we built this period	10
Missing-document reminders drafted from the portal's own list	10
The period's figures	11
Paid AI seats against active users	11
Credits used against the plan's allowance	11
Evidence register	12
References	14
Sign-off	15
Record	16

AI & Security Retainer

Riverbend Tax & Books

Engagement ID SG-RVB-2026-R1

Prior period	SG-RVB-2026-A1 · sha256 of that review's source document, not of this document: 7c85a72dd35fd03be367f03d32ec4e360ffb0877d6ea2221e78edaef2367f2eb
This period	SG-RVB-2026-A2 · sha256 of that review's source document, not of this document: 0c99ae155a15b0769dd01db93016bd01d5fc33f77c38e5dda8243ca9e96ad18b
Edition	Period 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 one period of the AI & Security Retainer. It sets this period's findings beside the prior period's. Both reviews used the same method. Each is named above with the fingerprint of its source file. To check a copy of either, drop the file itself on our Verify page, <https://stalwartgoverned.com/verify>. 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. Each row in the table states the difference between the two reviews, and nothing more. After the table come this period's coverage and the period's work: the visits, the maintenance and what was built, each with its evidence.

What held

Five findings from the prior period are resolved. Each was examined again this period and found in place and working. One finding is new this period.

	Risk area	Prior	This period	Change
P-01	An AI note-taker joining client calls	—	HIGH (D3×E3)	New
P-02	Client tax information pasted into a personal AI chat tool	CRITICAL (D4×E3)	—	Resolved
P-03	An AI tool that can learn from what is typed, with no data-processing agreement in place	CRITICAL (D4×E3)	—	Resolved
P-04	No second sign-in step on systems that hold client information	HIGH (D4×E2)	—	Resolved
P-05	Access not removed when people leave	HIGH (D4×E2)	—	Resolved
P-06	AI features switched on inside the tax software, with training terms unclear	HIGH (D4×E2)	—	Resolved

P-01 · An AI note-taker joining client calls

New — The prior review heard about this in interview but could not confirm it, so it was listed as a lead rather than a finding. This period's review confirms it.

HIGH (D3×E3) — same-day

What we found.

- **A2 · EV-13 · SCR** "an AI note-taker is connected to the shared calendar under a staff member's own account, and it joined two client advisory calls in September" — *calendar-integrations.png, connected apps*

- A2 · EV-21 · DOC "the register of data-processing agreements has no entry for the AI note-taker connected to the shared calendar" — *dpa-register.pdf, index*

Why it matters. Clients' personal and financial information is stored by a service the firm does not control. The firm has no data-processing agreement with that service. That puts client confidentiality at risk. The stored material could also be subject to discovery in a lawsuit.

What we would do.

- **Now.** Disconnect AI note-takers from client calls and from the shared calendar. This contains the problem.
- **Next.** Approve a transcription tool with a signed data-processing agreement that rules out training, or take notes by hand (this Retainer period).
- **Keep.** Check the apps connected to the calendar and meeting software at every monthly review (AI & Security Retainer).

Referenced: MEASURE 2.10 · LLM02

P-02 · Client tax information pasted into a personal AI chat tool

Resolved — Found at the prior review. We examined it again this period and found the control in place and working (A2 · EV-01).

What this period's review found.

- A2 · EV-01 · ADM "client cover letters are drafted only in the firm's own AI workspace, with learning from inputs off and deletion after 30 days; no consumer chat tool is signed in on any machine" — *ai-workspace-settings.png, data controls · captured 2026-09-21*

P-03 · An AI tool that can learn from what is typed, with no data-processing agreement in place

Resolved — Found at the prior review. We examined it again this period and found the control in place and working (A2 · EV-11).

What this period's review found.

- A2 · EV-11 · DOC "data-processing agreements are on file for the three AI services the firm has approved, including the renewed tax software, and each says customer data is not used for training" — *dpa-register.pdf, pp. 1–3 · captured 2026-09-21*

P-04 · No second sign-in step on systems that hold client information

Resolved — Found at the prior review. We examined it again this period and found the control in place and working (A2 · EV-02).

What this period's review found.

- A2 · EV-02 · ADM "the document-exchange portal still requires a second factor for every user, including the two staff who joined in September" — *portal-security-export.csv, all users · captured 2026-09-21*

P-05 · Access not removed when people leave

Resolved — Found at the prior review. We examined it again this period and found the control in place and working (A2 · EV-03).

What this period's review found.

- A2 · EV-03 · ADM "no enabled account belongs to anyone who has left; the leaver checklist was used for the one departure since the sprint" — *tax-users-export.csv, all rows · captured 2026-09-21*

P-06 · AI features switched on inside the tax software, with training terms unclear

Resolved — Found at the prior review. We examined it again this period and found the control in place and working (A2 · EV-04).

What this period's review found.

- A2 · EV-04 · DOC "the tax software contract renewed on 2026-09-15 with a data-processing addendum: client data is not used for training and is deleted on request; the assistant is back on under those terms" — *tax-renewal-addendum.pdf*, §2 · captured 2026-09-21

Coverage this period

This section lists what this period's review examined and what it did not. An area within the review's scope that it did not examine is listed here, so the lack of a finding there is never read as a clean result. The last rows are what the review saw in how the firm uses its tools. They are recorded as observations and are not graded.

Area	Status
Backups and tested restore	Examined — in place (A2 · EV-05).
Email domain authentication (SPF, DKIM and DMARC)	Examined — in place (A2 · EV-08).
AI features built into tax and bookkeeping software	Examined — in place (A2 · EV-04).
Managed security software on computers	Examined — in place (A2 · EV-06).
AI browser extensions and client information	Examined — in place (A2 · EV-12).
Multi-factor sign-in on systems that hold client information	Examined — in place for the document-exchange portal (A2 · EV-02).

Area	Status
Qualified Individual and written information security program	Examined — in place (A2 · EV-09).
Access removal when people leave	Examined — in place (A2 · EV-03).
Software updates	Examined — in place (A2 · EV-07).
Client information and personal AI chat tools	Examined — in place (A2 · EV-01).
Periodic review of third-party access	Examined — in place (A2 · EV-10).
AI vendor terms and data-processing agreements	Examined — in place for the three approved AI services (A2 · EV-11).
A written AI use policy, acknowledged by staff	Written, not followed (A2 · EV-17).
A shared library of prompts and templates, with a record of changes	Working well (A2 · EV-18).

Each row above was examined and names its evidence in the Evidence register. A row marked "in place" was found working. No area within this review's scope was left unexamined.

The period's work

What was done between the two reviews, and when. Where the review captured evidence of it, the line names the item in the register below.

Visits and calls

- 2026-09-15 — Joined Riverbend's renewal call with the tax software's maker. The data-processing addendum was signed on the call, and the assistant went back on for client files the same afternoon. (A2 · EV-04)
- 2026-09-21 — This period's review began on site: the systems that hold client data, the firm's written policies, and the AI tools in use.
- 2026-09-22 — The review finished with the staff walkthroughs, and its results were reviewed with the managing partner the same day.

Maintenance

- 2026-09-10 — A seasonal preparer left. The leaver checklist was worked through and every account was closed the same day. (A2 · EV-03)
- 2026-09-12 — The written information security program gained a section on the firm's AI tools, building on the vendor list added in the Sprint. The managing partner signed it as version 3.2. (A2 · EV-09)
- 2026-09-15 — The monthly restore check: the tax-software database restored to a test machine and checked against the live copy. (A2 · EV-05)
- 2026-09-17 — Two new staff joined. Each was set up with a second factor on the document-exchange portal on the first day, and their two new machines were enrolled in endpoint protection and automatic updates. (A2 · EV-02, A2 · EV-06, A2 · EV-07)

What we built this period

Each improvement below 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.

Missing-document reminders drafted from the portal's own list

What it is. The client portal's list of documents still missing for each return now feeds the firm's own AI workspace, which drafts a short reminder naming exactly what is outstanding. Each reminder cites the portal entry for every document it asks for. No reminder is sent until the office manager has checked it against the portal's list and read it through.

In use since 2026-09-16.

Who uses it. The office manager, in the weeks before each filing deadline.

What it saves. 14 minutes a client before the change, 5 after.

The timings, as captured.

- A2 · EV-19 · OBS "before the change, the office manager was timed writing reminders by hand to five clients whose returns were missing documents: 14 minutes a client" — *timing-notes.md*, §3 · captured 2026-09-08
- A2 · EV-20 · OBS "after the change, the office manager sent reminders to five clients from the portal's missing-document list, each drafted in the firm's own AI workspace citing the portal entry for every missing document, and checked against the portal's list before sending: 5 minutes a client" — *timing-notes.md*, §4 · captured 2026-09-19

The period's figures

What the firm pays for and what it uses, read off the vendors' own pages for this period. Each figure is printed as the page showed it, and nothing here is computed from them.

Paid AI seats against active users

Fully used — 4 seats paid for, 4 active in the period.

- A2 · EV-14 · FIN "the bookkeeping suite's invoice carries its assistant add-on on 4 seats" — *bookkeeping-invoice-sep.pdf, line 3 · captured 2026-09-22*
- A2 · EV-15 · ADM "the assistant add-on's usage report shows all 4 seats active in the trailing 30 days" — *assistant-usage.csv, 30-day view · captured 2026-09-22*

What this shows. A seat that is paid for and not signed into is a recurring charge for nothing. A seat used by more than one person is a shared login, which is a separate finding. The license page and the usage report, read together, show what the firm gets for that line of the invoice.

Credits used against the plan's allowance

Headroom — 300 credits in the cycle's allowance, 240 used.

- A2 · EV-16 · ADM "the assistant add-on's billing dashboard shows an allowance of 300 assistant credits in the cycle, with 240 used at capture" — *assistant-billing.png, cycle view · captured 2026-09-22*

What this shows. The plan's allowance is what the firm bought. The credits used are what it used. Credits left over every cycle point to a smaller plan. A cycle that runs over points to a bigger plan, or to a workflow worth reviewing. The figures are the vendor's own, read off its dashboard.

Evidence register

This register lists every piece of evidence this period's review captured, and where this record uses it. Each review numbers its own evidence, and A2 marks this period's review. This means A2 · EV-01 here is a different item from EV-01 in the audit or any other document. Each item's fingerprint is the first 16 characters of its source file's SHA-256, taken when the file was collected. To check a copy of a collected file, compute its SHA-256 and compare the first 16 characters. The full SHA-256 is kept with the engagement record.

	Code	Source	Fingerprint (first 16)	Used in
A2 · EV-01	ADM	ai-workspace-settings.png, data controls	9d0a6b7f74a2abd5	P-02; Coverage this period
A2 · EV-02	ADM	portal-security-export.csv, all users	4dbb7e40a16962dc	P-04; The period's work; Coverage this period
A2 · EV-03	ADM	tax-users-export.csv, all rows	cc763f2499f3d8c6	P-05; The period's work; Coverage this period
A2 · EV-04	DOC	tax-renewal-addendum.pdf, §2	1ee429c4fc934f7d	P-06; The period's work; Coverage this period
A2 · EV-05	LOG	backup-restore-log.txt, 2026-09-15	7d01845cf3c366d4	The period's work; Coverage this period
A2 · EV-06	ADM	endpoint-console.png, fleet view	9ada4bc2d0a9c5a7	The period's work; Coverage this period
A2 · EV-07	ADM	update-console.csv, all rows	0d45c4f61f80d630	The period's work; Coverage this period
A2 · EV-08	ADM	dns-records.txt, SPF · DKIM · DMARC	ddeb9eb321c9cdc8	Coverage this period

	Code	Source	Fingerprint (first 16)	Used in
A2 · EV-09	DOC	wisp-v3.2.pdf, §1, §7	c1cda71ff0e72fc4	The period's work; Coverage this period
A2 · EV-10	ADM	access-review-q3.pdf, p. 1	eda38c4b48d1e6f1	Coverage this period
A2 · EV-11	DOC	dpa-register.pdf, pp. 1–3	684548044dd9aa2e	P-03; Coverage this period
A2 · EV-12	ADM	extension-inventory.csv, all rows	0581b2fb8786f349	Coverage this period
A2 · EV-13	SCR	calendar-integrations.png, connected apps	d2b3e61e1ab428b8	P-01
A2 · EV-14	FIN	bookkeeping-invoice- sep.pdf, line 3	883529a5e66cee45	The period's figures
A2 · EV-15	ADM	assistant-usage.csv, 30-day view	f9e484147cb5022b	The period's figures
A2 · EV-16	ADM	assistant-billing.png, cycle view	681c9618dfb26558	The period's figures
A2 · EV-17	DOC	ai-use-policy-v2.pdf, p. 1	b209b48d34a6eb3d	Coverage this period
A2 · EV-18	SCR	prompt-library.png, version history	97b01f1c690e8a21	Coverage this period
A2 · EV-19	OBS	timing-notes.md, §3	fe3b4963aef7fc54	What we built this period
A2 · EV-20	OBS	timing-notes.md, §4	fe3b4963aef7fc54	What we built this period
A2 · EV-21	DOC	dpa-register.pdf, index	684548044dd9aa2e	P-01

References

Every framework code cited in the entries above, and the document it names. Statutes and regulations are named in full where they are cited.

- **MEASURE 2.10** — NIST AI Risk Management Framework 1.0: "Privacy risk of the AI system – as identified in the map function – is examined and documented."
airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF/Core_And_Profiles/5-sec-core
 - **LLM02** — OWASP Top 10 for Large Language Model Applications, LLM02:2025 Sensitive Information Disclosure: "Sensitive information can affect both the LLM and its application context. This includes personal identifiable information (PII), financial details, health records, confidential business data, security credentials, and legal documents." genai.owasp.org/llmrisk/llm022025-sensitive-information-disclosure/
-

Sign-off

Prepared by Peter Saar, CISSP #2450556.

AI & Security Governance · vCISO.

Issued by Stalwart Governed LLC.

This record states the difference between the two reviews named above, and nothing else. It is not a certification. A quiet period is not a promise about the next one.



STALWART GOVERNED

AI & Security Governance · vCISO

Engagement SG-RVB-2026-R1

Signed: Peter Saar · Date of issue: 2026-09-23



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-period.md	2f4983ee813a3d9e35bb2518a78cc7c255e40b2ec9e3ae78e6fd2e05e0d28ebf
length	226 lines · 16734 bytes
copy	1 of 1
version	d40fd37c5203 · cd154950a3cb
reference pack	2026-08-21
to check it	certutil -hashfile "riverbend-period.md" SHA256 (Windows) · shasum -a 256 "riverbend-period.md" (macOS) · sha256sum "riverbend-period.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.