

TECH & AI CASE STUDY - B2B SAAS - 2026

SOC 2 Type II in Five Months That Unblocked a \$4M Enterprise Pipeline

Based on a delivery engagement with Fernbrook Software

5 months

TIME TO SOC 2 TYPE II

\$4M

ENTERPRISE PIPELINE UNBLOCKED

-70%

QUESTIONNAIRE RESPONSE TIME

zero

AUDIT EXCEPTIONS

A fillable practice edition: the full story, 8 actions,
6 reflections and a 90-day plan - work it with your team.

Free - no email required
emersontechnology.com

MAKE THIS PRACTICE BOOK YOURS

Work it, do not just read it

This practice book turns the Fernbrook Software case study into a working session for your team. Read the full story first - what happened, what was built and what it changed. Then tick the 8 actions you can commit to, write short answers to the 6 reflections, and finish with a 90-day plan. Every field in this PDF is fillable: open it in Adobe Acrobat Reader, Chrome, Edge or macOS Preview, type directly into the boxes and save.

YOUR NAME

ROLE

COMPANY

TEAM / DEPARTMENT

DATE

EMAIL (OPTIONAL)

MY GOAL FOR THIS PRACTICE SESSION

- 01

The story - What happened at Fernbrook Software - before, during and after the project.
- 02

The results - The numbers that changed, plus industry benchmarks from public research.
- 03

The 8-action checklist - Tick boxes as your organization completes each step. Owner and date fields included.
- 04

The 6 reflections - Fillable questions that pressure-test your own roadmap.
- 05

My 90-day plan - Three fillable phase cards that turn this case study into your roadmap.

RUN IT AS A 90-MINUTE TEAM SESSION

25 min READ Read the story together. Ask everyone to note the one number that surprised them most.	40 min PRACTICE Work the 8-action checklist and the 6 reflections. Assign an owner and a date to every action you commit to.	25 min COMMIT Fill in the 90-day plan. One goal per phase, one number that tells you it worked. Book a review date before you leave the room.
--	--	---

THE STORY

What happened, and why it worked

01 The Company

Fernbrook Software is a 90-person B2B SaaS company whose platform helps mid-market logistics teams manage freight, warehousing and last-mile delivery. Its customers include shippers and third-party logistics providers, and its product sits squarely in the operational spine of those businesses: order flows, carrier rates, shipment status and the customer data attached to all of it. The company had found genuine product-market fit and was winning technical evaluations consistently — right up to the moment its deals reached procurement.

Enterprise procurement is where technical wins go to be audited. Fernbrook's target accounts were large enough that every vendor touching their operational data passed through a security review, and the review's gating question was almost always the same: provide your current SOC 2 Type II report. Fernbrook did not have one, and its improvised substitutes — a stale policy document, verbal assurances, screenshots assembled on request — were not moving deals forward. The company's growth story depended on converting a handful of named enterprise accounts, and every one of them was standing behind the same gate.

02 Where Things Stood

Three target accounts worth a combined \$4M in first-year contract value required a current SOC 2 Type II report, and two deals had already been lost to competitors over security review failures. Security policies lived in a stale Google Doc last meaningfully revised during a previous funding round. Evidence collection meant screenshots and guesswork: when a prospect asked for proof of access reviews or logging coverage, engineers reconstructed whatever they could find, and the result varied depending on who answered the email. Security questionnaires — each one 200 to 400 questions, each one overlapping the last — were answered ad hoc by whichever engineers had context, consuming days at a time and producing inconsistent answers that occasionally contradicted each other.

The founders understood the gap but feared the standard remedy. The prevailing wisdom among their peer founders was that a SOC 2 effort meant a multi-year audit slog that would freeze the product roadmap, consume the engineering manager's calendar and still end in an expensive report. Meanwhile the pipeline kept calling: the three target accounts represented expansion the board had already modeled, and procurement at each one had made the report a hard requirement rather than a preference. Leadership gave the team five months to produce the report or walk away from the pipeline, a deadline that reframed the project from "someday compliance work" into a product launch with a ship date.

03 The Challenge

The challenge was to take a 90-person company with zero formal controls and produce an unqualified SOC 2 Type II report in five months — without freezing the roadmap the business was betting on. The constraint eliminated every slow path: no leisurely policy-writing phase, no annual-cycle evidence gathering, no discovery of the auditor's calendar after the controls were built. Everything with a long lead time had to start in week one, and everything with a quality bar — evidence, reviews, incident response — had to be real, because auditors test whether processes operate rather than whether documents exist.

The scale of the ask is easier to see in context. IBM Security's 2024 research puts the global average breach cost at \$4.88 million, the highest figure the study has recorded, and finds that organizations making extensive use of security AI and automation save \$2.22 million per breach on average; Verizon's Data Breach Investigations Report has repeatedly found stolen credentials among the most common initial access vectors worldwide. Enterprise buyers were not inventing their requirements — they were reflecting genuine breach economics, and

Fernbrook needed controls that were defensible against that reality, not merely present in a document. The program had to produce operating evidence across five months, satisfy an independent auditor's sampling, and leave behind a compliance capability that would not collapse the moment the report was delivered.

04 Discovery and Diagnosis

Emerson Technology began with a two-week discovery that mapped Fernbrook's production environment, data flows and existing practices against the SOC 2 trust services criteria. The audit found a paradox common to strong engineering teams: many good practices already existed — encryption in transit, sensible cloud permissions, code review — but nothing was documented, owned, evidenced or consistent, and several controls the audit would sample had no process behind them at all. Access reviews had never been performed. Vendor risk files for subprocessors did not exist. Incident response was a channel in the team chat tool and goodwill. The diagnosis produced the three decisions that shaped everything after it. First, scope: the audit boundary would be drawn tightly around the core production environment and the customer data it touched, rather than boiling the ocean, because a tight scope cuts cost, effort and the number of controls to operate. Second, sequencing: the auditor had to be selected in week one — auditor availability, not engineering, is the most common cause of missed deadlines — with the observation window locked before controls were built. Third, mechanism: evidence would be collected by systems, not people. Each control would be mapped to the system that generates its proof, wired through APIs into a compliance automation platform, and verified daily by automated checks instead of annually by screenshots. The five-month plan was then backwards-scheduled from the observation window's start date.

05 The Solution

The program paired a compliance automation platform with hardened cloud controls, so that Fernbrook's audit evidence was generated by the environment itself.

A tight scope and an early auditor

The audit boundary was defined around the product's core production environment, keeping the scope small enough to operate but large enough to be honest — the environment where customer data actually lives. An auditor was selected in week one: three firms interviewed, fees agreed, and the 90-day observation window locked on the calendar before any control work began, which converted the deadline from a hope into a schedule. The window was kept deliberately compact with clean evidence from day thirty, meaning the observation period measured controls that were already operating rather than controls still being built.

Controls that check themselves daily

Roughly 60 controls were mapped to the SOC 2 trust services criteria in the compliance platform, each with a named owner, a defined test and evidence collection wired directly into cloud APIs. Terraform-managed guardrails enforced the encryption, logging and access baselines in code, so controls passed automated checks daily rather than annually — a control that fails on Tuesday is a ticket, while a control that fails in an audit is an exception. Access reviews ran on a monthly cadence from the first month, building the historical evidence auditors require while catching orphaned accounts within weeks instead of years. The platform became the system of record, and its dashboards replaced the screenshots that had previously stood in for proof.

The human evidence: vendors, reviews, response

The controls no API can generate were built in parallel. Vendor risk files were backfilled for every subprocessor — SOC 2 reports, data-flow diagrams and termination terms collected for each third party in the stack — because auditors sample vendors early and missing files generate avoidable exceptions. A tabletop incident response

exercise was run, written up and folded into an updated response plan, giving the auditor evidence the process actually works rather than a polished document that exists. Finally, a trust center was published for buyers: common security questions answered once, publicly, with the report available under NDA, so the sales team stopped consuming engineering time on overlapping questionnaires.

06 The First 90 Days

Week one closed the three long-lead decisions: scope, auditor and platform. Weeks two through six built the control framework — the 60-odd controls documented with owners and tests, the Terraform guardrails landing in the production repository, and the evidence integrations connected to the cloud provider, identity system and code repositories. By week six the automated checks were running daily, and the first failures surfaced exactly as intended: two logging gaps and a stale access grant, fixed within days, each fix generating its own evidence. Weeks seven through ten covered the operational controls that require lived history: the first two monthly access review cycles completed and archived, vendor risk files assembled subprocessor by subprocessor, and the incident response tabletop run with the engineering team, producing an after-action summary and a revised plan the auditor would later sample. The trust center went live in week ten, and the sales team answered its first enterprise questionnaire from maintained answers in hours instead of days. Weeks eleven through thirteen were stabilization: evidence pipelines monitored for gaps, controls failing any daily check remediated at the source, and the observation window opened with clean evidence flowing from day thirty as planned. By day 90, Fernbrook was operating its compliance program as a routine system, and the remaining two months of the observation window were simply the system running.

07 The Results

Fernbrook received an unqualified SOC 2 Type II report with zero exceptions in month five, and the \$4M in stalled enterprise contracts moved to signature within two quarters. Security questionnaires that consumed engineer days are now answered from a maintained trust center, cutting response time 70%, and two of the three target deals expanded mid-negotiation once the report cleared procurement. The platform now runs continuous compliance, so next year's audit is a review rather than a rebuild.

METRIC	BEFORE	AFTER
Time to SOC 2 Type II	-	5 months
Enterprise pipeline unblocked	-	\$4M
Questionnaire response time	-	-70%
Audit exceptions	-	zero

The durable change is that compliance became an engineering property rather than a sales emergency. Controls live in Terraform and pass daily checks, so the environment cannot quietly drift out of compliance between audits, and the monthly access reviews that once did not exist now generate the historical evidence every future audit will sample. Engineers stopped answering questionnaires ad hoc, recovering days of roadmap capacity each quarter. The founders' feared multi-year audit slog turned out to be a five-month build followed by a system that maintains itself — and the sales team now enters procurement conversations with the report attached instead of an apology.

08 What Your Business Should Do

The Fernbrook playbook works for any B2B SaaS facing its first enterprise audit, and its steps are mostly about sequence. Define the smallest defensible audit scope: draw the boundary around your core production environment and the data it touches, because a tight scope cuts cost, effort and the number of controls you must operate. Choose your auditor in week one — auditor availability, not engineering, is the most common cause of missed deadlines — so interview three firms early, agree fees, and lock the observation window before you build anything. Map controls to evidence sources first: for each control, identify the system that generates its proof and wire collection through APIs, because manual screenshots cannot survive a Type II observation window, let alone a daily automated check. Codify your baselines in infrastructure as code, enforcing encryption, logging and access rules through Terraform or equivalent tooling so controls pass automated checks daily instead of failing annual audits.

Run access reviews on a monthly cadence, because frequent lightweight reviews build the historical evidence auditors require and catch orphaned accounts within weeks rather than at annual cleanup time. Backfill vendor and subprocessor risk files — SOC 2 reports, data-flow diagrams and termination terms for every third party in your stack — since auditors sample vendors early and missing files generate avoidable exceptions that cost weeks. Exercise incident response before the window: run a tabletop, write the after-action summary and update the plan, because auditors want evidence the process works, not just a polished document that exists. Finally, publish a trust center for buyers — answer common security questions once, publicly, and link the report under NDA — because pre-built answers cut questionnaire turnaround from days to hours and shorten sales cycles. Sequence these eight steps against your own deadline with the action checklist in this practice book, and return to the reflection questions at every quarterly business review: how many enterprise deals stalled last year because you could not produce a current audit report, which of your controls would pass an automated daily check rather than a screenshot exercise, and what would a five-month audit freeze realistically cost your roadmap — is that cheaper than the pipeline you are losing?

REAL-WORLD PROOF & BENCHMARKS

IBM's 2024 Cost of a Data Breach report puts the global average breach cost at a reported \$4.88 million — the highest figure the study has recorded. - IBM Security, 2024

The same IBM report finds organizations making extensive use of security AI and automation reportedly save \$2.22 million per breach on average. - IBM Security, 2024

Verizon's Data Breach Investigations Report has repeatedly found stolen credentials among the most common initial access vectors in breaches worldwide, ahead of exploitation and social engineering. - Verizon DBIR, 2024

THE PRACTICE PAGES

The 8-action checklist

Work through the list with your team. Tick each box as your organization completes the step, and fill in an owner and a target date so every action has a name and a deadline.

☐

1. Define the smallest defensible audit scope

Draw the boundary around your core production environment and the data it touches. A tight scope cuts cost, effort and the number of controls you must operate.

OWNER

TARGET DATE

STATUS

--	--	--

☐

2. Choose your auditor in week one

Auditor availability, not engineering, is the most common cause of missed deadlines. Interview three firms early, agree fees, and lock the observation window before you build anything.

OWNER

TARGET DATE

STATUS

--	--	--

☐

3. Map controls to evidence sources first

For each control, identify the system that generates its evidence and wire collection through APIs. Manual screenshots cannot survive a Type II observation window, let alone a daily automated check.

OWNER

TARGET DATE

STATUS

--	--	--

☐

4. Codify baselines in infrastructure as code

Enforce encryption, logging and access rules through Terraform or equivalent tooling. Controls that live in code pass automated checks daily instead of failing annual audits.

OWNER

TARGET DATE

STATUS

--	--	--

☐

5. Run access reviews on a monthly cadence

Frequent lightweight reviews of application and cloud entitlements build the historical evidence auditors require. Monthly beats a frantic annual cleanup and catches orphaned accounts within weeks.

OWNER

TARGET DATE

STATUS

--	--	--



6. Backfill vendor and subprocessor risk files

Collect SOC 2 reports, data-flow diagrams and termination terms for every third party in your stack. Auditors sample vendors early, and missing files generate avoidable exceptions that cost weeks.

OWNER

TARGET DATE

STATUS

--	--	--



7. Exercise incident response before the window

Run a tabletop exercise, write the after-action summary and update the response plan. Auditors want evidence the process actually works, not just a polished document that exists.

OWNER

TARGET DATE

STATUS

--	--	--



8. Publish a trust center for buyers

Answer common security questions once, publicly, and link the report under NDA. Pre-built answers cut questionnaire turnaround from days to hours and shorten sales cycles.

OWNER

TARGET DATE

STATUS

--	--	--

AFTER THE CHECKLIST: OUR TOP 3 PRIORITIES

From the eight actions above, write down the three you will start first - and the single number you expect each one to move. Three priorities with owners beat eight without any.

PRIORITY 1 NUMBER IT SHOULD MOVE	PRIORITY 2 NUMBER IT SHOULD MOVE	PRIORITY 3 NUMBER IT SHOULD MOVE
--	--	--

THE PRACTICE PAGES

Reflections for your team

Use these questions in your next planning session and type short answers into the boxes. The gaps you find are usually the fastest wins.

Q1. How many enterprise deals stalled in the last year because you could not produce a current audit report?

Q2. Which of your controls today would pass an automated daily check rather than a screenshot exercise?

Q3. If procurement demanded your SOC 2 report next week, how long would your team need to respond?

Q4. How much engineer time goes into answering overlapping security questionnaires every quarter?

Q5. Do you know every subprocessor touching customer data, and could you produce their audit reports today?

Q6. What would a five-month audit freeze realistically cost your roadmap — and is that cheaper than the pipeline you are losing?

THE PRACTICE PAGES

My 90-day plan

Finish the session by committing to a plan. Three phases, one goal each, one number that tells you it worked. Bring this page to your next leadership review - or to a free consultation with Emerson Technology, and we will pressure-test it with you.

Days 1-30 Focus: audit and alignment

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 31-60 Focus: build and prove

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 61-90 Focus: scale and measure

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Tip: save a copy per team so each group keeps its own answers. Revisit the reflections every quarter - the questions stay the same even as the numbers move.

BOOK THE REVIEW BEFORE YOU CLOSE THE BOOK

Plans without a review date drift. Before you close this practice book, agree on when you will come back to these pages, who will run that session, and when you will check the numbers again. If you want an outside pair of eyes, bring this page to a free consultation with Emerson Technology and we will pressure-test the plan with you.

REVIEW DATE	REVIEWED BY	NEXT CHECK-IN
------------------------------------	------------------------------------	--------------------------------------

Ready for a transformation like Fernbrook Software's?

Emerson Technology designs and builds the data, AI, cloud and automation systems behind results like these. On a free consultation call we will map this exact playbook to your business - your data, your constraints, your numbers.

Book a free consultation

support@emersontechnology.com

or start online: emersontechnology.com/contact