

A DIAGNOSTIC FOR LEADERS

The Tech Leverage Audit

**Is your technology multiplying your team or
taxing it?**

A 35-question diagnostic for CEOs, founders and investors who run a technology-dependent business but don't have a technical leader they fully trust to tell them how it's really going.

BY

Bryan Dennstedt

Fractional CTO and Chief AI Officer

bry.net/tech-audit

Take it as a 5-minute quiz



The quiet tax on growth

Very few CEOs wake up and think, "we have a technology problem." They think the team is slow, the vendor is expensive, or the roadmap keeps slipping.

SOUND FAMILIAR?



Every release takes longer than promised, and "it's more complicated than we thought" has become normal.



Engineering spend keeps climbing while the amount that ships stays flat.



One developer or one agency holds the keys, and everyone knows it.



A simple question like "which customers are most profitable?" turns into a project.



You're quietly dreading the day an investor or acquirer asks for technical due diligence.



Everyone agrees you should be using AI. Nobody owns it.

Each of those looks like its own problem. Usually they share a cause: the technology was built to get the company to here, and nobody has stepped back to decide what it needs to get the company to there.

Adding developers rarely fixes it. More people on a shaky foundation means more coordination, more rework and a bigger bill. The fix starts with seeing clearly where the drag is coming from.

HERE

The technology that got you this far

THE DRAG

Slower releases, rising cost, key-person risk, messy data

THERE

The technology your next stage needs

Good technology makes a small team look big. Weak technology makes a big team feel small.

BRYAN DENNSTEDT

How to use this audit

The audit looks at seven areas a CEO can judge without reading a line of code. Each one has a short explanation, the warning signs to look for, one question to ask your team, and five statements to score.

- 01**  **Strategy Fit** The technology plan follows the business plan.
- 02**  **Architecture and Scale** The platform can grow without a rewrite.
- 03**  **Delivery** Work ships when you're told it will.
- 04**  **Team and Key-Person Risk** The business doesn't depend on one person or one vendor.
- 05**  **Data** You can trust your numbers and get answers fast.
- 06**  **Security and Diligence Readiness** You'd pass a review tomorrow.
- 07**  **AI Leverage** AI is doing real work, with an owner and a result.

The scoring rule

Give yourself 1 point for each statement that is clearly true today. If you have to think about it, or the honest answer is "sort of," it doesn't count.

THE STEPS

1. Read each section and score its five statements (0 to 5).
2. Add the seven sections together (0 to 35).
3. Find your band on the scoring page.
4. Start with your lowest section, using the "What to fix first" table.

Pro tip

Better yet, score it twice: once yourself, and once with your technical lead or vendor. Where your answers differ is where the real conversation is.



bry.net/tech-audit

Prefer a quiz? Scan to score it online and get your results instantly.



Strategy Fit

The technology plan follows the business plan.



STRATEGY

ARCHITECTURE

DELIVERY

TEAM

DATA

SECURITY

AI

Your tech roadmap should read like a translation of your business goals. If the company is chasing a new market, a bigger customer or a lower cost to serve, the technology work should visibly point at it.

When strategy fit is weak, engineering stays busy on whatever is loudest: the latest customer request, the founder's newest idea, or a rewrite someone has wanted for years. The team works hard and the business barely moves.

WARNING SIGNS

- › The roadmap is a list of features with no business goal attached to each one.
- › Priorities change whenever a big customer or the loudest voice asks.
- › Nobody can say what the technology needs to look like in 18 months.
- › Tech decisions happen in the engineering channel, not at the leadership table.

WHAT GOOD LOOKS LIKE

- ✓ Every big piece of tech work traces back to a named business goal.
- ✓ Leadership can say no to a project without a fight, because the plan already decided.
- ✓ The 18-month picture is written down and gets revisited every quarter.

ASK YOUR TEAM

"If we hit our revenue goal next year, what breaks first?"

SCORE YOURSELF

 1 point for each statement that is clearly true

- ☐ Our technology roadmap ties every major initiative to a specific business goal.
- ☐ Leadership and the tech team agree on the top three technology priorities for this year.
- ☐ We have a written view of what our technology needs to support 18 to 24 months from now.
- ☐ We regularly say no to technical work that doesn't move the business forward.
- ☐ Someone with technical judgment has a real seat at the leadership table.

STRATEGY FIT SCORE _____ / 5

Scored 0 to 2? Start here: Write a one-page technology strategy that maps the next 12 months of tech work to the business plan, and review it at leadership meetings.

02 Architecture and Scale

The platform can grow without a rewrite.



STRATEGY

ARCHITECTURE

DELIVERY

TEAM

DATA

SECURITY

AI

Architecture is the shape of your system: how the pieces fit, where data lives, and how hard it is to change one part without breaking another. You don't need to understand the diagram. You do need to know whether it can carry twice the load.

Weak architecture shows up as fragility. Small changes cause surprise outages, performance dips at your busiest moments, and the team starts talking about "starting over." A full rewrite is one of the most expensive decisions a company can make, and it is usually avoidable when caught early.

WARNING SIGNS

- › The system slows down or falls over during your busiest periods.
- › Small changes regularly break something unrelated.
- › "We need to rebuild it" comes up more than once a quarter.
- › Your hosting bill grows faster than your customer count.

WHAT GOOD LOOKS LIKE

- ✓ Doubling customers is a capacity question with a known answer and a known cost.
- ✓ Changes stay contained: fixing one thing doesn't break three others.
- ✓ The fragile parts are known, named and on a plan to be fixed.

ASK YOUR TEAM

"What would happen if we doubled our customers next month?"

SCORE YOURSELF

1 point for each statement that is clearly true

- ☐ We could handle twice our current customers or volume without a major rebuild.
- ☐ Changes to one part of the product rarely break something unrelated.
- ☐ Our hosting and infrastructure costs grow slower than our revenue.
- ☐ We know which parts of the system are the most fragile, and there is a plan for them.
- ☐ Our technology choices are mainstream enough that we can hire for them.

ARCHITECTURE AND SCALE SCORE _____ / 5

Scored 0 to 2? Start here: Get an outside architecture review that names the three biggest scale risks and a sequenced plan to fix them without a rewrite.

03 Delivery

Work ships when you're told it will.



STRATEGY

ARCHITECTURE

DELIVERY

TEAM

DATA

SECURITY

AI

Delivery is the heartbeat of a technology team: how reliably ideas become working software in customers' hands. Healthy teams ship small pieces often, and they tell you about trouble before the deadline, not after it.

When delivery is weak, every date is a guess and every launch is a fire drill. Sales stops promising features, customers stop believing roadmaps, and leadership loses the ability to plan.

WARNING SIGNS

- › Deadlines slip so often that nobody plans around them anymore.
- › Releases are big, rare and stressful events.
- › You find out about problems on launch day.
- › Bugs customers report keep coming back.

WHAT GOOD LOOKS LIKE

- ✓ Small releases go out every week or two, and they're boring.
- ✓ Dates come with a range and a confidence level, and they mostly hold.
- ✓ Bugs are caught before customers find them, and fixed fast when they aren't.

ASK YOUR TEAM

"What did we ship to customers in the last two weeks?"

SCORE YOURSELF

1 point for each statement that is clearly true

- ☐ Most work ships within a reasonable range of the date we were given.
- ☐ We release improvements to customers at least every two weeks.
- ☐ We hear about risks to a deadline early, while there is still time to adjust.
- ☐ Releases are routine, not all-hands emergencies.
- ☐ We track a few simple delivery measures, such as time to ship and bugs found by customers.

DELIVERY SCORE _____ / 5

Scored 0 to 2? Start here: Move to small, frequent releases with a weekly demo of what shipped, and track two or three simple delivery measures leadership can read.

04

Team and Key–Person Risk

The business doesn't depend on one person or one vendor.



STRATEGY

ARCHITECTURE

DELIVERY

TEAM

DATA

SECURITY

AI

Many growing companies run on a hero: the first developer, a founder who codes, or a long-time agency. Heroes are valuable. A business that can't function without one is fragile.

Key-person risk is the one investors ask about first, because it is the easiest way for a company to lose a year. If the knowledge lives in one head, every vacation, resignation or contract dispute becomes a crisis.

WARNING SIGNS

- › One person is the only one who can deploy, fix or explain a critical system.
- › Your agency or contractor owns accounts, code or passwords you don't control.
- › Documentation is "ask Sam."
- › New hires take months to become useful.

WHAT GOOD LOOKS LIKE

- ✓ Any one person can take a two-week vacation without the business noticing.
- ✓ The company owns every account, repository and domain, with logins on file.
- ✓ New engineers ship something real in their first two weeks.

ASK YOUR TEAM

"If our lead developer quit on Friday, could we still ship next month?"

SCORE YOURSELF 1 point for each statement that is clearly true

- ☐ If our most important technical person left tomorrow, we could keep shipping within a few weeks.
- ☐ The company, not a vendor or an individual, owns every code repository, domain, cloud account and admin login.
- ☐ How our core systems work and how to deploy them is written down somewhere the team uses.
- ☐ New engineers can make a useful change in their first two weeks.
- ☐ Our vendors and contractors have clear deliverables and are held to them.

TEAM AND KEY-PERSON RISK SCORE _____ / 5

Scored 0 to 2? Start here: Run an ownership and access audit, move every account and repository into company control, and document the critical paths so no one person is a single point of failure.

05 Data

You can trust your numbers and get answers fast.



STRATEGY

ARCHITECTURE

DELIVERY

TEAM

DATA

SECURITY

AI

Your data is a record of everything customers do with you. When it is clean and connected, leaders can answer real questions in minutes: who is about to churn, which product line makes money, where the funnel leaks.

When data is weak, every report starts an argument about whose spreadsheet is right. Decisions get made on instinct because the facts take too long to assemble. Data is also the fuel for any serious AI effort, so weak data quietly caps what AI can do for you.

WARNING SIGNS

- › Two reports on the same question give two different answers.
- › Key numbers live in someone's personal spreadsheet.
- › Simple questions take days and an engineer to answer.
- › Customer data is scattered across tools that don't talk to each other.

WHAT GOOD LOOKS LIKE

- ✓ Leadership questions get answered in minutes from one trusted source.
- ✓ Customers, revenue and usage are defined once and mean the same thing everywhere.
- ✓ The data is clean enough to feed AI tools without a cleanup project first.

ASK YOUR TEAM

"How long would it take to tell me our ten most profitable customers?"

SCORE YOURSELF

1 point for each statement that is clearly true

- ☐ We have one trusted source for our key business numbers.
- ☐ Leaders can answer common business questions without asking an engineer.
- ☐ Our main systems (product, CRM, billing, support) share data instead of living in silos.
- ☐ We know what customer data we hold, where it lives and who can see it.
- ☐ Our data is clean and organized enough to power reporting or AI tools.

DATA SCORE _____ / 5

Scored 0 to 2? Start here: Define the ten numbers that run the business, give each one a single source of truth, and connect your core systems so those numbers update on their own.



Security and Diligence Readiness

You'd pass a review tomorrow.



STRATEGY

ARCHITECTURE

DELIVERY

TEAM

DATA

SECURITY

AI

Security used to be an IT topic. Now it is a sales and valuation topic. Larger customers send security questionnaires, insurers ask hard questions, and every investor or acquirer runs technical due diligence.

Weak security rarely shows until the worst moment: a breach, a lost enterprise deal, or a diligence report that knocks real money off a valuation. The basics are not glamorous, and they are far cheaper to fix before someone else finds them.

WARNING SIGNS

- › Security questionnaires from customers cause a scramble.
- › Former employees or contractors may still have access to systems.
- › There is no tested backup or plan for a major outage.
- › Nobody has looked at your licenses, open-source use or compliance obligations.

WHAT GOOD LOOKS LIKE

- ✓ A security questionnaire takes days, and the answers are already written.
- ✓ Access is removed the same day someone leaves.
- ✓ A diligence request list would be an afternoon of gathering, without a scramble.

ASK YOUR TEAM

"If an acquirer started technical due diligence on Monday, what would worry you?"

SCORE YOURSELF 1 point for each statement that is clearly true

- ☐ Multi-factor login is required on every critical system, and access is removed the day someone leaves.
- ☐ Backups are tested, and we have a written plan for a major outage or breach.
- ☐ We can answer a customer security questionnaire in days, not weeks.
- ☐ We understand our compliance obligations (for example HIPAA, SOC 2 or PCI) and are meeting them.
- ☐ An outside party has reviewed our security or code within the last year.

SECURITY AND DILIGENCE READINESS SCORE _____ / 5

Scored 0 to 2? Start here: Close the basics first (logins, access removal, tested backups), then build a diligence-ready folder that answers the questions investors and enterprise customers always ask.

07 AI Leverage

AI is doing real work, with an owner and a result.



STRATEGY

ARCHITECTURE

DELIVERY

TEAM

DATA

SECURITY

AI

Most companies are already using AI. Their employees just aren't telling anyone. Unmanaged AI use creates risk (sensitive data pasted into public tools) and wastes the opportunity, because good ideas stay in one person's browser tab.

Strong AI leverage looks boring in the best way: a short list of specific uses, each with an owner, a measured result and clear rules about data. Weak AI leverage looks like a lot of excitement, a few pilots and nothing anyone can point to.

WARNING SIGNS

- › AI comes up in every meeting, and nothing has shipped.
- › Employees use personal AI accounts with company data, and nobody has set rules.
- › Pilots start, then fade without a decision.
- › Nobody can say what AI has saved or earned the company so far.

WHAT GOOD LOOKS LIKE

- ✓ Each AI use has an owner, a measured result and a clear data rule.
- ✓ People use approved tools on purpose, with training, and say so out loud.
- ✓ The next three AI bets are ranked by business value, with a test for each.

ASK YOUR TEAM

"Where is AI saving us time or money today, and how do we know?"

SCORE YOURSELF 1 point for each statement that is clearly true

- ☐ We have at least one AI use in production that saves measurable time or money.
- ☐ Each AI initiative has a named owner and a way to measure success.
- ☐ We have clear, simple rules for what company data can and can't go into AI tools.
- ☐ Our team has company-approved AI tools and training to use them well.
- ☐ We have a short, prioritized list of where AI could help next, ranked by business value.

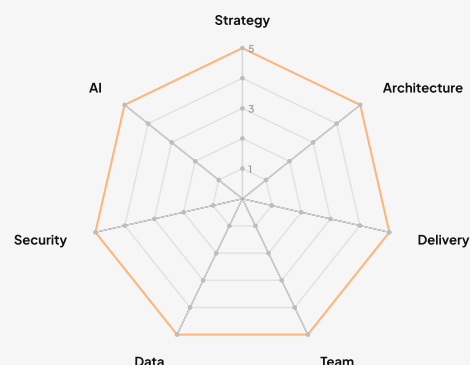
AI LEVERAGE SCORE _____ / 5

Scored 0 to 2? Start here: Approve the tools, set simple data rules, then pick two high-value uses with an owner and a 90-day target, and measure them.

Scoring your audit

01	Strategy Fit	_____	/5
02	Architecture and Scale	_____	/5
03	Delivery	_____	/5
04	Team and Key-Person Risk	_____	/5
05	Data	_____	/5
06	Security and Diligence Readiness	_____	/5
07	AI Leverage	_____	/5
Total		_____	/35

PLOT YOUR SHAPE



Mark each score on its spoke and connect the dots. The dents show where to start.

Putting Growth at Risk
0 to 13

Creating Drag
14 to 20

Working, but Fragile
21 to 28

A Force Multiplier
29 to 35

29 to 35

A Force Multiplier

Your technology is helping a small team punch above its weight.

Protect it. Close the remaining gaps, keep the plan tied to the business, and look for the next place AI can add leverage.

21 to 28

Working, but Fragile

Things mostly work, but a few weak spots are carrying more risk than they look.

This is where many growing companies sit. One resignation, one big customer or one diligence request can turn a weak spot into a crisis.

14 to 20

Creating Drag

Technology is slowing the business down in ways the team is working around.

Your people are compensating with extra hours, heroics and workarounds. That works until it doesn't, and it costs more every quarter.

Under 14

Putting Growth at Risk

The foundation probably can't support the growth you're asking it to carry.

Adding people or features right now will likely add cost faster than progress. Step back, get an outside view and set a plan before the next big push.

What to fix first

Every area connects to the others, so the work eventually touches all seven. Start with your lowest score. That's where the drag is costing you the most right now.



If Strategy Fit is weak

Write a one-page technology strategy that maps the next 12 months of tech work to the business plan, and review it at leadership meetings.



If Architecture and Scale is weak

Get an outside architecture review that names the three biggest scale risks and a sequenced plan to fix them without a rewrite.



If Delivery is weak

Move to small, frequent releases with a weekly demo of what shipped, and track two or three simple delivery measures leadership can read.



If Team and Key-Person Risk is weak

Run an ownership and access audit, move every account and repository into company control, and document the critical paths so no one person is a single point of failure.



If Data is weak

Define the ten numbers that run the business, give each one a single source of truth, and connect your core systems so those numbers update on their own.



If Security and Diligence Readiness is weak

Close the basics first (logins, access removal, tested backups), then build a diligence-ready folder that answers the questions investors and enterprise customers always ask.



If AI Leverage is weak

Approve the tools, set simple data rules, then pick two high-value uses with an owner and a 90-day target, and measure them.

The goal is leverage. Technology should let a small team do big things. When the strategy, the platform, the people and the data line up, every hire and every dollar goes further. When they don't, the business pays a quiet tax on everything it tries to do.

ABOUT THE AUTHOR

Bryan Dennstedt

Fractional CTO and Chief AI Officer

I have 28+ years building and fixing technology for growing companies, mostly seed to Series B in healthtech, AI and SaaS. I sit on your side of the table: helping you decide what to build, who to hire, what to say no to, and how to tell the technology story to your board and your buyers.

I also host the AI with Bry podcast, where I talk with operators about putting AI to work in real businesses.

HEALTHTECH, ACQUIRED

Modernized an at-home health-testing platform and led the security and due-diligence work that made it acquirable. Acquired by Recuro Health in 2021.

HEALTHCARE AI

Turned a clinical-AI startup's broad mission into a focused use case and a story buyers could act on.

He knew how to work with healthcare clients and their corporate constraints, and how to turn our mission into something the market could actually buy.

SHEILA PANDE, CEO, TANDEM

The next step is yours.

Did this audit surface a gap? Let's talk through your score.

bry.net/contact



bry.net/tech-audit

Score it online