OKC CIO PARTNERS · FREE GUIDE

The Oklahoma Small Business Technology Guide 2026

A vendor-neutral playbook for IT strategy, security, and AI — built for small and mid-sized businesses across the Oklahoma City metro.

Grey Lawson
Founder & Fractional CIO, OKC CIO Partners
grey@okcvcio.com · (405) 209-6071 · www.okcvcio.com

INTRODUCTION

Why this guide exists

Most small and mid-sized businesses in the Oklahoma City metro are stuck between two bad options: keep running IT reactively — fixing what breaks, one emergency at a time — or hire a full-time IT director for $200,000-plus a year you can't justify. This guide is the middle path: the decisions a chief information officer would make for you, in plain terms you can act on this quarter.

It is deliberately **vendor-neutral**. Nothing in here is selling you a product, a platform, or a managed-services contract. The goal is to help you make better technology decisions whether or not we ever work together.

How to use it

Each chapter follows the same shape: the problem, what "good" actually looks like, and two or three things you can do right now. If all you have is five minutes, read the bronze callout in each chapter — that's the version I'd give you over coffee.

A note on AI

AI runs through this whole guide, because it runs through how I work. I operate my own practice on AI-augmented workflows, so I'll be straight with you about where it saves real time and where it's a distraction wearing a tie.

CHAPTER 1 · STRATEGY

Start with a roadmap, not a wish list

The most expensive technology decisions are the ones made reactively. A server dies, so you buy whatever is fast. A tool frustrates someone, so you sign up for another. Twelve months later you have a stack nobody chose on purpose and a budget full of surprises.

A 12-month IT roadmap fixes that. It turns technology from a cost center that ambushes you into a plan you control — sequenced, budgeted, and tied to where the business is actually going.

What good looks like

- A short list of initiatives, each tied to a business goal — not a generic best-practices checklist.
- Every initiative carries a cost, a risk, and a rough timeline, so leadership can prioritize with eyes open.
- It’s reviewed quarterly and adjusts as the business changes.

Do this now

- Write down your top three business goals for the year.
- For each, ask: “What does technology need to do to support this?” That list is the start of your roadmap.

> **THE TEST OF A REAL ROADMAP**
>
> It’s sequenced and budgeted. If everything is priority one, you don’t have a roadmap — you have a wish list, and the loudest emergency wins every time.

CHAPTER 2 · SECURITY

Own the risk before it owns you

Two-thirds of ransomware incidents now hit companies with fewer than 500 employees. You are not too small to be a target — to an attacker running automated tools, you are the *easy* target.

Here's the part most owners miss: businesses rarely get breached because they bought the wrong tool. They get breached because **no one owns the risk**. The MSP patches and monitors. Leadership assumes security is handled. In reality it's not handled — it's simply unassigned.

What good looks like

- A plain-English risk register: what could hurt the business, how badly, and what to fix first — ranked.
- Multi-factor authentication everywhere that matters: email, remote access, and admin accounts.
- Backups that are tested, and security controls that actually match what your cyber-insurance policy requires.

Do this now

- Confirm MFA is enforced on email and any remote access.
- Ask your MSP for the date of your last *successful* backup restore test.
- Pull out your cyber-insurance policy and read the control requirements you attested to.

> **THE INSURANCE TRAP**
>
> Most cyber policies require specific controls. If you attested you have them and you don't, the claim gets denied at the worst possible moment — after the breach. Make reality match the policy now, not during a claim.

CHAPTER 3 · RESILIENCE

Plan for the bad day

A backup you have never restored from is a hope, not a plan. The difference between a ransomware attack that costs you an afternoon and one that costs you a quarter is decided long before the attack — in whether your recovery was designed and rehearsed.

In 2020, ransomware hit a multi-site business I ran IT for. We were back in about two hours, no ransom paid, because the backups were air-gapped and the recovery plan was real. Most firms in that position lose weeks.

What good looks like

- At least one backup copy that is air-gapped or immutable — offline, where ransomware can’t reach it.
- Defined RTO and RPO per system: how fast you must be back, and how much data you can afford to lose.
- A written recovery runbook someone has actually walked through.

Do this now

- Define an RTO and RPO for your most critical system — the one that stops the business if it’s down.
- Schedule a real restore test this quarter. Not a backup check — an actual restore.

> **THE FIVE-MINUTE VERSION**
>
> Online backups get encrypted right alongside everything else. Keep one copy offline or immutable, and test that you can actually restore from it. That single discipline is what bought us two hours instead of two weeks.

CHAPTER 4 · FOUNDATION

Get Microsoft 365 and the cloud right

For most SMBs, Microsoft 365 is the backbone — email, files, and identity in one place. Done well, it's one of your strongest security assets. Done lazily, it's an open door with your whole business behind it.

And not everything belongs in the cloud. Cloud where it earns its keep, on-prem where it makes sense — including the ERP and line-of-business systems some Oklahoma operations genuinely depend on.

What good looks like

- Conditional Access and MFA enforced; a small, controlled number of global admin accounts.
- Endpoints managed (e.g., with Intune) so a lost laptop isn't a lost database.
- Licensing right-sized to what you actually use.

Do this now

- Count your global admin accounts. If it's more than two or three, that's your first project.
- Review your license tiers — most SMBs are paying for capabilities they don't use, or missing security features they already own.

> **A LICENSE AUDIT USUALLY PAYS FOR ITSELF**
>
> The same Microsoft 365 subscription often includes security controls businesses are paying a third party to duplicate. Knowing what you already own is free money.

CHAPTER 5 · VENDORS

Stop herding vendors

Your MSP keeps the lights on, and the good ones are very good at it. But an MSP is not, structurally, your advisor — its revenue grows when you buy more *from the MSP*. When the company selling the solution also tells you whether you need it, the advice can never be fully independent.

Meanwhile your support provider, software vendors, ISP, and security tools each have their own contact, contract, and finger-pointing. When something breaks across them, the business owner becomes the middleman. That's not your job.

What good looks like

- One person independently owns vendor selection, contract review, renewal negotiation, and MSP accountability.
- Contracts stay in your name — no markup, no commissions, no referral fees in the middle.
- Every vendor, renewal date, and annual cost lives in one place you can see.

Do this now

- Build a one-page list: every IT vendor, what it costs per year, and when it renews.
- Flag every auto-renewal. Ask your MSP for an SLA / performance report.

> **WHERE THE MONEY HIDES**
>
> One bad auto-renewing contract often costs more in a single year than independent oversight of your whole vendor stack would. The renewals just quietly charge while no one is watching.

CHAPTER 6 · BUDGET

Make IT spend predictable

IT spend should be a plan, not a series of surprises. When budgeting is reactive, you overpay in emergencies and underinvest everywhere else — the worst of both.

What good looks like

- A capital and operating IT budget that separates “keep the lights on” from “change the business.”
- A hardware refresh cycle, so aging equipment is replaced on a schedule instead of at failure.
- A simple ROI expectation on project spend, and licenses reviewed for waste.

Do this now

- Split this year’s IT costs into run-the-business vs. change-the-business.
- Set a refresh cycle (commonly 3–5 years) for endpoints and servers, and put the replacements in the budget before they fail.

KNOW ONE NUMBER

IT spend as a percentage of revenue. The right figure varies by industry, but if you can’t state yours, that’s the first problem to solve — you can’t manage what you don’t measure.

CHAPTER 7 · AI

Use AI where it saves real time

AI is genuine leverage and a genuine distraction, depending entirely on where you point it. I run my own practice on AI-augmented workflows, so this isn't theory for me — it's how the work gets done.

Where it saves real time

- Drafting and editing, summarizing long documents, and routine customer communication.
- Answering questions over your own files and data — and routine analysis that used to eat afternoons.

Where it's a distraction

- Chasing hype, or an "AI strategy" with no specific workflow attached.
- Any tool where you can't answer a simple question: where does our data go?

One risk hides in plain sight: if your team is pasting client or company data into public chatbots, that's **shadow AI** — a confidentiality problem you may never see. The fix isn't a ban, which just drives it underground. It's a sanctioned tool that's faster and safer than the workaround.

> **DON'T BUY "AI"**
>
> Buy back hours on one specific task. Pick a single repetitive workflow, pilot AI on it, and measure the time saved. Then do the next one. That's how AI pays for itself instead of becoming shelfware.

CHAPTER 8 · COMPLIANCE

Get the compliance basics right

Compliance frameworks look intimidating from the outside and are mostly the same thing on the inside: a defined set of security controls, plus evidence that you actually follow them. The ones most Oklahoma SMBs encounter:

- **HIPAA** — if you handle protected health information (medical, dental, and many of their vendors).
- **CMMC** — if you're in the defense supply chain.
- **SOC 2** — if you're a SaaS or service provider whose clients ask how you protect their data.
- **PCI DSS** — if you take card payments.

What good looks like

- You know which frameworks actually apply to you — and which don't.
- A gap analysis against the real requirements, and a remediation roadmap with owners and dates.
- Evidence kept continuously, not reconstructed in a panic the month before an audit.

> **THE SHORTCUT NOBODY ADVERTISES**
>
> Compliance is mostly a byproduct of good security plus good documentation. Build the posture first and the audit gets dramatically easier — chasing the certificate without the posture underneath is how businesses fail both.

SELF-ASSESSMENT

Your 10-minute IT self-assessment

Answer these honestly. They map to the eight chapters you just read.

01	**Do you have a written IT roadmap that looks 12 months ahead?**	Yes / No / Not sure
02	**Is MFA enforced on email, remote access, and admin accounts?**	Yes / No / Not sure
03	**Do you have a plain-English risk register, reviewed with leadership?**	Yes / No / Not sure
04	**Has a backup been successfully *restored* (not just run) in the last 90 days?**	Yes / No / Not sure
05	**Is at least one backup copy air-gapped or immutable?**	Yes / No / Not sure
06	**Do your security controls match what your cyber-insurance policy requires?**	Yes / No / Not sure
07	**Do you know how many Microsoft 365 global admin accounts you have?**	Yes / No / Not sure
08	**Is there one place listing every IT vendor, cost, and renewal date?**	Yes / No / Not sure
09	**Do you know your IT spend as a percentage of revenue?**	Yes / No / Not sure
10	**Is there a sanctioned, safe way for your team to use AI?**	Yes / No / Not sure
11	**Do you know which compliance frameworks apply to your business?**	Yes / No / Not sure
12	**Is there one person — independent of your vendors — who owns these answers?**	Yes / No / Not sure

HOW TO READ YOUR SCORE

If you answered “No” or “Not sure” to three or more, you have gaps that are worth a conversation — and almost certainly worth more than a conversation costs. The last question is the one that quietly drives all the others.

WHERE TO GO FROM HERE

You don’t need a $200K hire. You need the seat filled.

I’m Grey Lawson. I’ve spent 28 years in IT — 24 of them as an IT Director running complex, multi-site environments. I started OKC CIO Partners because the Oklahoma City metro is full of businesses that need executive-level technology leadership but can’t justify a full-time CIO, and whose only other option is an MSP happy to sell them more.

How the engagement works

I sit in the strategic seat **above** your day-to-day support. Your MSP or in-house staff keeps doing what it does best; I own the roadmap, the risk, the budget, and the vendors — and I’m your single point of accountability at CIO altitude.

1. Free discovery call. 60–90 minutes. We talk about your business and whether there’s a fit. No deck, no pitch.
2. Paid IT assessment. A written risk summary and a prioritized 12-month roadmap — the foundation everything else is built on.
3. Month-to-month retainer. Fractional CIO leadership, no long-term contract. If I’m not delivering, it takes one email.

My promise

Vendor-neutral, always. I don’t resell hardware, software, or managed services. No markups, no commissions, no referral fees. I select your vendors and negotiate your contracts, but they stay in your name — so my only compensation is my fee, and when I tell you that you *don’t* need something, there’s nothing on my invoice arguing otherwise.

START THE CONVERSATION

Book a free discovery call at okcvcio.com, email grey@okcvcio.com, or call (405) 209-6071. Serving Oklahoma City, Edmond, Norman, Moore, Yukon, Mustang, Guthrie, Midwest City, and the surrounding metro — on-site and remote.