CLOUD READINESS GUIDE

What's Still on Your Server?

Most businesses are far less "in the cloud" than they think. Here is how to find out in twenty minutes.

At some point your business moved email to Microsoft 365. Maybe you moved the practice management system, or the EHR, or the case management platform to a hosted version. Somebody said "we're in the cloud now" and everyone moved on.

Meanwhile, there is still a box in a closet. It holds scanned records, shared drives, an old line-of-business application, the backup nobody has tested, and the permissions structure that nobody has reviewed since the person who built it left. **That box is the part of your business that is still exposed, still aging, and still on a replacement clock you are not tracking.**

This guide is a working inventory. Go through it, check the boxes, count your flags, and use the summary on the last page to bring the answer to whoever signs off on it.

> **HOW TO USE THIS**
> Check every item that is still running on a physical server or a workstation in your office, or that you honestly cannot answer. Uncertainty counts as a flag. Not knowing where client or patient data lives is the finding, not a gap in the exercise.

PART ONE: THE INVENTORY

Six Categories, Twenty-One Questions

Flags are weighted by what happens if the item fails or gets breached, not by how hard it is to move.

1. Files and Documents	6 items
☐ A mapped network drive (S:, X:, the "shared" drive) If it only works in the office or over VPN, it is not cloud storage.	HIGH
☐ Scanned records, intake forms, or closed matters Usually the largest pile of regulated data and the least protected.	HIGH
☐ Imaging, recordings, or large media files Commonly excluded from backup because of size. Check whether yours is.	HIGH
☐ Templates, forms, and firm or practice standards Low risk, high daily friction. First thing people email to themselves.	LOW
☐ Files saved to individual desktops rather than a shared location Almost never backed up. Walks out the door with the laptop.	HIGH
☐ Anyone using a personal Dropbox, Google Drive, or USB drive for work files Shadow storage. You have no visibility, no logs, and no way to revoke it.	HIGH

2. Applications and Line-of-Business Software

4 items

- [ ] **An application that only runs when you are physically in the office** — HIGH
  Billing, imaging, document management, an old database, a custom tool.
- [ ] **Software the vendor no longer actively supports or updates** — HIGH
  No patches means no fix when a vulnerability is published.
- [ ] **A hosted platform that still needs an on-prem component to work** — MEDIUM
  A local print service, scan bridge, or database connector. Very common.
- [ ] **An application nobody has confirmed a cloud version exists for** — MEDIUM
  In most cases one does now. The assumption is usually years out of date.

3. Backup and Recovery

4 items

- [ ] **Backups live in the same building as the server** — HIGH
  A fire, a flood, or a burst pipe takes both. This is Florida.
- [ ] **Nobody has performed a test restore in the last twelve months** — HIGH
  An untested backup is a hope, not a recovery plan.
- [ ] **You cannot say how long a full recovery would take** — HIGH
  If the answer is "a few days," price a few days of lost revenue.
- [ ] **Microsoft 365 data is assumed to be backed up by Microsoft** — HIGH
  It is not. Microsoft protects the platform. Your data retention is on you.

> **THE NUMBER THAT MATTERS HERE**
>
> Average ransomware downtime is 24 days (Statista). Fifty-eight percent of businesses hit by ransomware in 2024 closed their doors (Huntress). The question is not whether you have a backup. It is whether anyone has proven it comes back.

4. Identity and Access

4 items

- [ ] **You cannot produce a list of who has access to what** — HIGH
  This is the first thing an auditor, a carrier, or a client asks for.
- [ ] **Offboarding takes more than one business day** — HIGH
  A single failure here cost one medical center $111,400 in HIPAA penalties.
- [ ] **Multi-factor authentication is not enforced on every account** — HIGH
  "Most accounts" is the same as none for insurance purposes.
- [ ] **Shared logins exist for any system** — HIGH
  A shared login means your audit log cannot name a person.

5. Remote and Mobile Access

3 items

- [ ] **Working from home requires a VPN or a remote desktop session** — MEDIUM
  Slow, fragile, and the thing that fails the night before a deadline.
- [ ] **Staff use personal devices with no management or encryption on them** — HIGH
  If that phone or laptop is stolen, what is on it and can you wipe it?
- [ ] **Someone has to drive to the office to print, scan, or retrieve a file** — LOW
  Count how many times a month. That is pure lost payroll.

6. The Physical Box Itself

4 items

- [ ] The server is more than five years old, or you do not know its age — **HIGH**
  Past five years you are running on borrowed time and expired warranty.
- [ ] It sits in a closet, a storage room, or under someone's desk — **HIGH**
  No climate control, no physical access control, no camera.
- [ ] There is no line item in next year's budget to replace it — **MEDIUM**
  The bill is coming whether it is planned or not.
- [ ] One person understands how it is configured — **MEDIUM**
  If that person leaves or gets sick, you have a single point of failure with a pulse.

PART TWO: YOUR SCORE

Count Your Checked Boxes

Twenty-one possible flags. Most businesses that believe they are "in the cloud" land in the middle band.

0 to 4 flags Genuinely cloud-first

You are in good shape. The work left is tuning: right-sizing licenses, tightening permissions, and confirming your backup and retention actually covers Microsoft 365. Skip to the licensing section on the next page.

5 to 11 flags Half migrated, which is the most common place to be

You moved the obvious things and stopped. What remains holds the regulated data, has no redundancy, and carries the replacement cost. Your provider is probably telling you everything is fine, and technically it is: the server runs, backups report success, nothing is on fire. What is not being said is that you are on a clock and cannot prove your compliance posture on paper. This is the most expensive place to sit.

12 or more flags Mostly on-premise

Your business depends on hardware in a room in your office. Not a crisis today. It becomes one the day the box fails, the building floods, or someone encrypts it. Treat the next twelve months as a planned migration instead of waiting for an unplanned one.

IF YOU DECIDE TO ACT

What Typically Moves First

Nobody moves everything at once. This order reduces the most risk fastest.

Phase	What Moves	Why This Order
Weeks 1 to 2	Identity and files. MFA everywhere, shared drives to SharePoint	Cheapest and fastest. Closes the biggest gaps first
Weeks 2 to 4	Backup and devices. M365 backup, device management, encryption	Protects what you just moved, and proves it on paper
Next quarter	The line-of-business application, then retire the server	The hardest piece, done last for a reason

PART THREE: THE MONEY

The Server You Already Own Is Not Free

What a five-year cycle actually costs a business of 25 to 75 people.

Cost Line	Typical Range	What Usually Gets Missed
Server hardware	$6,000 to $12,000	Replaced every 5 years, not amortized in anyone's head
Server OS and client access licenses	$1,200 to $4,000	Repurchased at every refresh
Backup appliance and software	$1,500 to $4,000	Its own hardware, on its own replacement cycle
Battery backup and replacements	$600 to $1,500	Batteries die every 3 to 4 years and rarely get tested
Power and cooling, 5 years	$2,000 to $4,500	Buried in the electric bill, never attributed to IT
Patching, monitoring, and maintenance	$3,000 to $9,000	Either billed by your provider or paid in staff time
Five-year total	**$14,300 to $35,000**	**Before a single hour of downtime**

AND THEN THE DOWNTIME

Employees lose 91 hours a year to IT issues (Robert Half). For a 40-person office that is roughly 3,600 hours of paid time spent waiting on technology. None of it appears on an invoice.

THE COMPARISON

Where the Cost Actually Goes

Category	Server in the Closet	Cloud-First
Replacement cost	Large capital expense every 5 years, timing not yours to choose	None. No hardware to refresh
If hardware fails	Down until parts arrive. Days, not hours	No single box to fail
Access from anywhere	VPN or remote desktop, slow and fragile	Native from any device, same speed everywhere
Audit trail	Usually not configured. Often not possible	Built in. Exportable for auditors and carriers
Offboarding a departing employee	Manual, multi-system, easy to miss something	One action, logged, same day
Hurricane or building loss	You lose the hardware and everything on it	Staff work from anywhere the next morning

Being blunt: if you are still on a local server with no business case for it, you are about ten years behind. That is not a sales pitch, it is where the market is.

PART FOUR: LICENSING

The July 2026 Price Increase Changed the Math

Microsoft raised business plan prices on July 1, 2026. One plan did not move, and that changes what you should be buying.

Plan (month-to-month, per user per month)	Before	Now	Change
Microsoft 365 Business Basic	$7.20	$8.40	+16%
Microsoft 365 Business Standard	$15.00	$16.80	+12%
Microsoft 365 Business Premium	$26.40	$26.40	No change
Microsoft 365 F1 (frontline)	$2.70	$3.60	+33%
Microsoft 365 F3 (frontline)	$9.60	$12.00	+25%
Microsoft 365 E3	$43.20	$46.80	+8%
Microsoft 365 E5	$68.40	$72.00	+5%

Pricing shown is month-to-month, which is what most businesses should be on for a portion of their seats. Annual commitment runs roughly 20% lower per license but locks the seat for the full term. Existing subscriptions keep prior pricing until the first renewal on or after July 1, 2026.

The part almost nobody caught

Business Premium held flat at $26.40 while Standard went from $15.00 to $16.80. The gap between them shrank from $11.40 to $9.60 per user per month. Premium is the tier that carries device management, conditional access, advanced threat protection, and the access logging you need when an auditor or a malpractice carrier asks you to prove something. For under ten dollars a month, on the people who actually handle regulated data, that is now one of the easiest security decisions available to a small business.

What we actually recommend

Stop licensing everyone the same way. That is the single most common and most expensive mistake we see. Match the license to the role: Premium for the people who handle patient records, client files, or financial data on a mobile device. Standard for general office staff. Basic or Exchange-only for people who genuinely just need email and a calendar. Frontline plans for shift workers who share a workstation and rarely touch a desktop app. Most offices we audit are carrying 10 to 20 percent more licenses than they have people, and nearly all of them are one tier too high on half the staff.

WHILE YOU ARE IN THERE

Check for licenses still assigned to people who no longer work for you. If your provider is not reconciling seat counts every month, nobody is. We have never audited an environment and found zero unassigned or orphaned licenses.

What you should be paying for a Microsoft license

Exactly what Microsoft charges. Four Winds passes vendor pricing straight through, includes license management at no additional cost, and reconciles your seat count monthly. If your invoice shows a license fee, a platform base fee, and a per-seat management fee, you are paying three charges for one thing.

PART FIVE: THE OBJECTIONS

Four Fair Questions, Answered Straight

These come up in every one of these conversations. They deserve real answers, not reassurance.

"What happens when the internet goes down?"

The fair answer is that you add a second path. A business-class primary connection with cellular failover on the firewall runs roughly $50 to $150 a month and switches over in seconds. Files synced through OneDrive and SharePoint stay available on the device and sync back when you reconnect, so people keep working through an outage. Worth sitting with: your server has no failover either. When it dies, there is no second path. You are down until replacement hardware physically arrives.

"Our compliance requirements won't allow cloud."

They almost certainly do. HIPAA permits cloud storage of protected health information with a signed Business Associate Agreement, and Microsoft signs one. Bar ethics opinions across states have permitted cloud storage of client data with reasonable safeguards for well over a decade. In practice the closet server is usually the weaker compliance position, because you cannot produce access logs, prove encryption at rest, or document who opened what and when. Cloud platforms generate that evidence by default. Your server generates it only if someone configured it to, and usually nobody did.

"We can't afford the disruption."

For a business of 25 to 75 people, a file and infrastructure migration runs two to four weeks. Data copies in the background over nights and weekends while everyone keeps working on the current system. The cutover itself happens on a weekend. Most staff notice a different drive letter on Monday and a short training session. The disruption people picture is the unplanned version: the server fails, and you take whatever downtime the hardware lead time gives you.

"It costs more every month."

Monthly, usually yes. Over five years, usually not, once the refresh cycle, licensing, backup hardware, power, and maintenance are counted honestly. The real difference is shape. You trade unpredictable capital hits that land when hardware decides, for a predictable monthly number that scales with headcount. Finance people tend to prefer that trade once they see it laid out.

What we will tell you honestly

Sometimes the answer is to wait. If your server is two years old, your application genuinely has no cloud version, and your risk exposure is low, we will tell you to plan for it at refresh rather than spend money now. We would rather be right than busy.

TAKE THIS INTO YOUR NEXT REVIEW

Five Questions to Ask Your Current IT Provider

If the answers are vague, that is the answer.

- [ ] "What is still running on hardware in our building, and what happens if it fails tonight?"
- [ ] "When did you last run a verified test restore, and can you show me the result?"
- [ ] "Are we backing up Microsoft 365 separately, or are we assuming Microsoft handles it?"
- [ ] "How many licenses are we paying for, and how many are assigned to people who still work here?"
- [ ] "What would it cost and how long would it take to get the rest of this off our server?"

TEAR THIS PAGE OFF

Summary for Leadership

Fill this in and bring it to whoever signs off. One page, no jargon, decision at the bottom.

Total flags out of 21	______ Band: ______
The systems still running on our own hardware	______
Year our server was purchased	______ Age today: ______ years
Last verified test restore of our backup	______
Is replacement in next year's budget?	Yes ☐ No ☐ Don't know ☐
Estimated 5-year cost of staying as-is	$ ______
What we are recommending	______
Decision we need from you	______

FOR THE PERSON SIGNING OFF

Three Questions to Ask Before You Approve Anything

1. If that server died tonight, what is our answer tomorrow morning?

If nobody can answer in a sentence, you do not have a recovery plan. You have a backup that somebody believes in.

2. If an auditor, a carrier, or a client asked who accessed a specific file last month, could we show them?

"We trust our team" is not the answer any of those three are looking for.

3. What is this decision going to cost us in the year we do not make it?

The refresh, the downtime, and the risk do not go away when the decision gets deferred. They just get less predictable.

Want us to check your work?

Send us your completed inventory and we will send back a findings summary with a cost estimate and a recommended sequence.

Within 48 hours. No charge, no meeting required, no obligation to do anything with it.

Send Your Inventory

info@fourwindsit.com | (941) 315-2380 | fourwindsit.com