

The No-Doors Checklist

A twenty-minute audit for whether your business runs without you standing in the doorway.

My dad came to every game I ever played, except the one where I hit my only home run. He'd stepped away for a cup of coffee. That was still the standard I grew up on, and it's the standard I built my company around: be there, and let the business keep running anyway.

Nobody can lock the doors on a company that has no doors. That only holds if everything the business needs is reachable from more than one place, by more than one person, without one building, one device, or one person having to say yes first. Cloud tools are the mechanism. Portability is the actual rule.

This is the twenty-minute version of that audit. It is not a technology checklist. It is a permission checklist. Every question is really asking one thing: if you couldn't show up tomorrow, could someone else reach what they need to keep the lights on. Most owners who run it find at least one gap they assumed was already covered.

This is the audit I built to run against my own business in about twenty minutes. It won't catch everything. It catches the obvious gaps, and those are the ones that sink people, because everyone assumes somebody else already checked them.

1 The One Question

Every item below asks the same thing a different way: who, besides you, keeps this piece of the business running if you're not reachable. If the honest answer is nobody, you've found a door with exactly one key. Where you can't check the box, that's the item you fix on a Tuesday afternoon instead of on the worst day of the year.

2 Cloud-Native Access

Cloud-native isn't a technology decision. It's a location decision. If a file lives only on one computer or in one drawer, the business lives there too.

SYSTEM	REACHABLE FROM ANY DEVICE, ANY SECURE SIGN-IN, NO SINGLE BUILDING OR MACHINE REQUIRED	CHECK
Client files and records	No local-only folder, no "just this once" exception	
Contracts and agreements	Stored where more than one person can pull them up	
Invoicing and accounting	Reachable without waiting on one specific machine	
Calendar	Same version, visible to everyone who needs it	
Passwords and credentials	Live in a system built for it, not a head or a sticky note	

One clarification. Cloud-native doesn't mean owned. Every tool on this list is rented, the same as a filing cabinet would be. The cloud changes whether you can reach it and whether you can leave it. It doesn't change what you're standing on.

3 Single Source of Truth

It isn't enough to have things in the cloud. You need exactly one place each thing lives. Two systems that quietly disagree isn't redundancy. It's a coin flip, and you won't know which side it landed on until the answer needs to be right.

- ☐ **One calendar.** Not a master copy and a second version an assistant keeps somewhere else.
- ☐ **One place client records live.** Not a notebook only one person can read.
- ☐ **One place contracts and promises live.** Not buried across three people's inboxes.
- ☐ **One place passwords live.** Not in your head, and not on paper in one building.
- ☐ **One record of what you told a client.** Written down the same day, in the place client promises belong.

4 The Rehearsed Export Test

Every tool you rent will tell you that you can export your data any time you like. Almost none of them make you actually try it until the day you need to leave, the wrong day to find out the export button is broken. An export you've never opened is a hope, not a plan. Portability you've never rehearsed is borrowed, wearing rented's name tag.

- 1 **List every tool the business genuinely depends on.**
If losing it for a week would hurt, it's on the list.
- 2 **Once a year, click export on each one.**
Not "someday." Put a date on the calendar and keep it.
- 3 **Open the file and read it.**
Confirm it holds what you think it holds, in a format a replacement tool can read without starting from a blank screen.
- 4 **Actually restore from it.**
Walk the rebuild path start to finish, the way you'd have to on the real day. Almost everyone skips this step, and it's the one that proves the other three meant anything.

5 Credential Map and Admin Redundancy

This is the boring one, and it's also the one that reopens the doors when something goes wrong. The person who registered the domain leaves and nobody wrote the login down anywhere else. A solo owner has a medical emergency and for two weeks nobody else can get into the accounting software. Neither is a technology failure. Both are documentation failures, preventable with an afternoon and a password manager built for teams.

SYSTEM	SOMEONE BESIDES YOU HAS STANDING ADMIN ACCESS, TODAY	CHECK
Domain and hosting	Not just you know the login	
Bank and accounting	A trusted second person can get in without waiting on you	
Email and core client system	Access exists now, not as a promise to share it later	

Give at least one other person, a partner, a co-owner, a trusted assistant, live access, not a promise. Check the map once a year, the same week as the export tests. Logins rot the same way old exports do: quietly, and only once you go looking.

6 Portability Is Not Permissiveness

No Doors means access doesn't depend on one place or one device. It does not mean security gets turned off. A door only one key opens is a risk. Data only one password protects is that same risk, wearing a different name tag.

- ☐ **Multi-factor sign-in** on every system that touches client data or money.
 - ☐ **Encryption** on data at rest, not just in transit.
 - ☐ **Access revoked the day someone rolls off.** Not three months later when someone remembers.
 - ☐ **A regulated-industry carve-out, if it applies to you.** Health, finance, and defense already regulate where data lives and who can touch it. Those rules win. Build your version of No Doors inside them, with someone qualified signing off.
-

WHAT THIS IS. A thinking tool for finding your own gaps, not IT, security, or legal advice, and not a substitute for a real risk assessment from someone qualified to run one. As of July 2026, verify any rule about data handling, encryption, or regulated-industry requirements with your own counsel or compliance advisor before relying on it.

HOW TO USE THIS. This is a thinking tool, built to help you reason about your own firm. It is not a compliance guarantee and it is not legal advice. Where it states a rule, it states the rule as of 2026-07, and the law moves, so confirm the current rules in your jurisdiction with your own counsel before you rely on anything here.

From *The Automated Law Firm* • 4Spot Consulting • [HTTPS://JEFF-ARNOLD.COM/BUILD-WHAT-CANT-BE-TAKEN/THE-NO-DOORS-CHECKLIST/](https://JEFF-ARNOLD.COM/BUILD-WHAT-CANT-BE-TAKEN/THE-NO-DOORS-CHECKLIST/)