

DCBKK 2026 · YOUR WORKSHEET



# Staying Sane When Everything Keeps Shifting

Know in seven minutes which risk to fix first.

One risk, one owner, one date. Everything else in this guide is here when you need it.

---

1 **What could go wrong?**

Stuck? Try: your main AI tool or platform is gone, a serious flaw appears in a system you rely on, or your files or logins disappear.

---

2 **Business impact?**

---

3 **What protects us today?**

---

4 **Tested or assumed?**

☐ TESTED

☐ ASSUMED

---

5 **Next action** Write it as: when X happens, I do Y.

---

6 **Owner: one name** A name, not a department. Have clients? One sheet per key client.

---

7 **Who does the work** A person, a role or an AI tool.

---

8 **Proof it is done, and the date**

---

---

If I do only one thing this week, it is:

---

Each month, turn one Assumed into Tested.

Filled-in example, two prompts and tools for your developer:  
[byjed.com/dcbkk26notes](https://byjed.com/dcbkk26notes)

FROM THE TALK

# Four moves keep you calm when the ground shifts

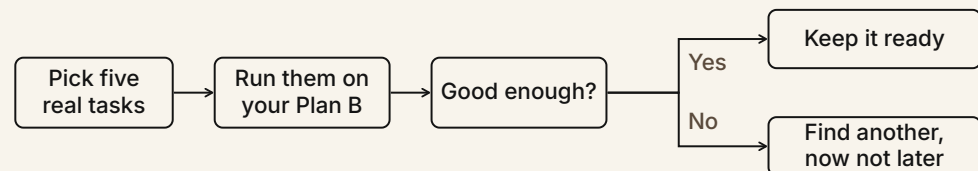
One small step for each move. Do it on a quiet day.

I

DEPENDENCY

## Test your Plan B

Run real tasks on your Plan B before you need it.



ASK If this provider disappears tomorrow, what happens?

2

RUNNING FINE

## Check what an outsider can reach

When a piece of your product or website is badly out of date, ask three questions: can an outsider reach it, is there a fix and who owns it, and how do we know the fix worked?

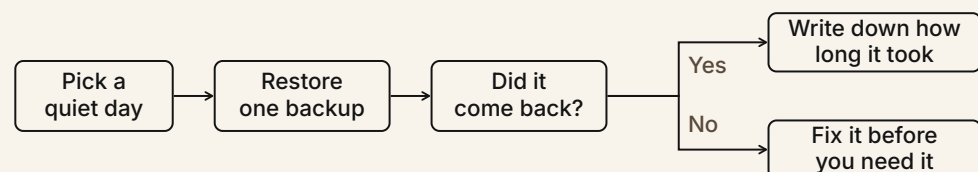
ASK Are any of our building blocks badly out of date?

3

RECOVERY

## Prove the recovery

Restore one backup on purpose, on a quiet day. A backup you have never restored is a hope, not a plan.



ASK If something disappears, can we restore it?

4

ACCESS

## Keep the damage small

Give tools view-only access (can read, cannot change). Make the tool ask you before anything that deletes.

ASK If a tool goes wrong, what can it damage?

You don't need to predict everything that will change. You need a business that can absorb change without falling apart.

## THE FIRST HOUR

## If something goes wrong

A bad day is easier when the first hour is already decided.

|                                   |                                            |                                         |                                  |                                    |
|-----------------------------------|--------------------------------------------|-----------------------------------------|----------------------------------|------------------------------------|
| 1                                 | 2                                          | 3                                       | 4                                | 5                                  |
| Unplug it from the live business. | Cancel the API keys and passwords it used. | Keep the evidence, change nothing else. | Call the one person who owns it. | Write down what happened and when. |

If you do not hold the API keys yourself, make the call (step 4) first.

## DAILY HYGIENE

## Small, boring, every week. Like brushing your teeth.

Seven habits that cover most of it. Most take a few minutes.

|                     |                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| WEEKLY              | Check that automatic updates ran on phone, laptop, browser and the building blocks of your product.                                     |
| ONCE                | Use a password manager, one password per place, and two-step login on email, bank, domain and hosting. Email first: it resets the rest. |
| QUARTERLY           | Restore one backup to prove it works.                                                                                                   |
| WHEN SOMEONE LEAVES | Cancel their keys the same day. Keep one list of who holds keys: people, tools, API keys.                                               |
| EVERY TIME          | Take ten seconds before you scan, paste or install. Who made it, who sent it, what will it touch?                                       |
| EACH NEW TOOL       | Give it a visitor pass. It may read. Changing, paying or sending asks a human.                                                          |
| QUARTERLY           | Put your owner list on the wall, so everyone knows who to call.                                                                         |

### The phishing links of today

|                |                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------|
| THE OLD RULE   | Do not click a link from a sender you do not know. It worked because you can read where a link goes before you click. |
| THE NEW SHAPES | A QR code, a pasted prompt or an add-on from GitHub does not show you what is inside.                                 |
| SAME RULE      | Who sent it, who made it, what will it be allowed to touch? Same rule for your team and your family.                  |

## YOUR CHECKLIST

# Your two paths

Pick your path, then tick only what you have proof for. Most founders need only one.

## A You work with a developer or agency

Ask them these questions. Get the answers in writing.

- ☐ Which of our systems do you watch? Who checks whether a new security warning affects our setup?
- ☐ How does an urgent issue reach me, and how fast do you confirm you saw it?
- ☐ Who reviews, fixes and checks each issue? What do I see as proof the fix worked?
- ☐ Which backups exist? When did someone last restore one, and how long did it take?
- ☐ If a change breaks the live product, how do we go back to the last good version?
- ☐ If our main AI tool, platform or host is unavailable, what happens to the business?
- ☐ Which logins, API keys or AI tool permissions could do serious damage, and how are they limited?
- ☐ Where are our API keys and passwords kept, and who can see them? If one leaks, how fast can we cancel it?

**What counts as proof:** a restore test with a date and a time taken. A fix checked on the live product, not only in the code. A return to the last good version that someone has actually done. A monthly report is not enough for an urgent issue.

## B You build it yourself with AI tools

Check before you put changes live, and after big changes.

- ☐ **Permissions.** The AI tool starts view-only (can read, cannot change). It asks before anything that deletes or touches the live product.
- ☐ **Review first.** The tool proposes the change, you read it, then it goes live.
- ☐ **Small changes.** One change at a time, so you can see what broke and undo it.
- ☐ **Tests.** A few real examples you run after every change, with a clear idea of good enough.
- ☐ **Backups.** Keep a second copy somewhere else, and one copy that nobody can change or delete from your live system. Restore once to prove it works.
- ☐ **API keys and passwords.** Keep them out of code, chats and logs. If one leaks, cancel it and make a new one.
- ☐ **Security checks.** Check the live product, not only the code.
- ☐ **A way back.** You know how to return to the last good version, and you have done it once.
- ☐ **A simple plan.** Who you call and what you do first, written down before you need it.

**Remember:** an AI tool that says "done" has not proved anything. A passing test, a working restore and a check of the live product are proof.



### Jed Tabaczynski

I run engineering teams and build products on AI tools for a living, after years as a consultant.

[jed@byjed.com](mailto:jed@byjed.com)

[linkedin.com/in/tabaczynski](https://linkedin.com/in/tabaczynski)

[byjed.com](https://byjed.com)

Questions about your sheet are welcome. Want a free outside check of what anyone on the internet can spot on your product? Email me with CHECK and your domain. Only domains you own or have written permission to check.