The Internal Systems Risk Checklist

Twenty questions that surface the operational risk hiding in your spreadsheets, automations, AI tools, and internal workflows.

Roshan Mishra — roshanmishra.in

These are the same questions I ask at the start of every Internal Systems Risk Audit. Answer them honestly. If three or more make you wince, that is usually a sign an audit would pay for itself quickly.

Spreadsheets and manual systems

1. Is there a spreadsheet that, if it broke or someone overwrote a formula, would stop a core part of your business — billing, leads, delivery — for more than a day?

2. Does more than one person edit that spreadsheet with no validation, access control, or version history?

3. Is there a real backup of your core operational data that isn't "someone's laptop"?

4. Has a spreadsheet error ever produced a wrong number that reached a client, an invoice, or a report?

Automations and workflows

5. Do you have an automation running (Zapier, Make, n8n, Google Apps Script) that nobody on the team could explain step-by-step today?

6. If that automation failed silently tomorrow, how would you find out — and how long would it take?

7. Do your automations have error handling, logging, or an alert for when something breaks?

8. Is there a workflow that only works because one person manually checks or fixes it every week?

AI tools

9. Do you have an approved list of AI tools your team is allowed to use for client work?

10. Has anyone on your team pasted client or company data into a consumer AI tool without asking first?

11. Do you know what data your current AI tools store, and where it goes?

12. Could you answer a client's or insurer's questions about your AI usage today, in writing?

Access and credentials

13. Are any business-critical accounts — domain, hosting, banking, main email — owned by a personal address instead of a company one?

14. Is there a single, current record of who has access to what: logins, API keys, admin panels?

15. Has anyone who left the company in the last two years kept access to anything?

16. Do you know exactly what happens to your systems if the person who set them up is unreachable for a week?

Documentation and key-person risk

17. If your most operationally knowledgeable person left tomorrow with no notice, could someone else run the business for a week?

18. Are there written, current SOPs for your core recurring processes — or does the knowledge live in one person's head?

19. Is there a video or written walkthrough for how to operate your most critical system?

20. When was the last time anyone reviewed your tools and subscriptions for what's outdated, unused, or redundant?

If three or more of these made you wince, that's a good place to start.

Book a Systems Risk Audit: roshanmishra.in/contact

Email: roshanmis@gmail.com