FREE RESOURCE / XBITIUM SECURITY

NIST Cybersecurity Framework — Gap Checklist

The famous framework, translated into questions you can actually answer.

The NIST Cybersecurity Framework (CSF 2.0) is the most widely recognised way to describe a security programme — and it is increasingly quoted at small businesses by clients and insurers who want to know you have one. The official documents are dense. This checklist restates each of the six CSF functions as plain questions. Mark each **Yes**, **Partly**, or **No**. Every 'No' and 'Partly' is a gap to close.

WHAT CHANGED IN CSF 2.0

The 2024 update added **GOVERN** as a sixth function, sitting alongside the original five (Identify, Protect, Detect, Respond, Recover). It recognises that security is a leadership responsibility, not merely an IT task — which is exactly the mindset a small business needs.

G. Govern

Is someone actually in charge of security?

Yes	Partly	No	Question
			Is one named person accountable for security decisions?
			Do you have written security policies, even short ones?
			Is there a budget (time or money) allocated to security?
			Do you know which laws and standards apply to your data?

ID. Identify

Do you know what you are protecting?

Yes	Partly	No	Question
			Do you have a list of your devices, systems, and software?
			Do you know where your sensitive and customer data lives?
			Have you assessed your top security risks? (see our worksheet)
			Do you know which suppliers can access your data?

PR. Protect

Are the safeguards actually in place?

Yes	Partly	No	Question
			Is multi-factor authentication enabled on key accounts?
			Are systems and software kept patched and up to date?
			Is access limited to what each person actually needs?
			Do staff receive security awareness training regularly?
			Is data encrypted on laptops and in transit?
			Are backups running, and have you tested a restore?

DE. Detect

Would you even notice an attack?

Yes	Partly	No	Question
			Is endpoint protection installed, and are its alerts monitored?
			Do you review logs, or have something that flags the unusual?
			Do you scan for vulnerabilities more than once a year?
			Do staff know how to recognise and report suspicious activity?

RS. Respond

Do you have a plan for the bad day?

Yes	Partly	No	Question
			Do you have a written incident response plan? (see our template)
			Does everyone know who to call, and is it written down?
			Do you know your legal breach-notification obligations?

RC. Recover

Can you get back to business?

Yes	Partly	No	Question
			Can you restore operations from clean backups?

			Have you actually tested recovery, not just assumed it works?
			Do you capture lessons learned and fix the root cause?

TURNING GAPS INTO A PLAN

Count your 'No' answers — that is your gap list. Do not try to fix them all at once. Pull them into the Risk Assessment Worksheet, score each one, and work the highest scores first. Steady progress beats a heroic weekend that burns you out.

WHEN YOU WANT TO KNOW WHAT IS ACTUALLY EXPOSED

A checklist tells you what *should* be true. A scan tells you what *is* true. Xbitium will scan your public-facing systems and send you a real report in 48 hours — free, nothing to install, no obligation. If you are in good shape, we will say so and leave you alone.

Request your free external scan at xbitiumsecurity.com