



Law Firms

IT & Cyber Resilience Checklist

A practical checklist for solicitors, chambers,
and specialist legal practices

MANAGE. PROTECT. ASSURE.

Purpose of this checklist

A senior read on your IT and cyber posture

Law firms hold confidential and privileged client data and handle client money, which makes them one of the most targeted sectors for cyber attack and fraud. The SRA expects firms to prevent, detect and respond, and clients and insurers increasingly ask for proof. These questions are written to help you identify the gaps between what you believe is in place and what you could actually prove.

Why this checklist matters

- Remote working, cloud services and external suppliers have widened the ground you need to defend
- Law firms are a top target for email and payment fraud, especially around property completions
- The SRA expects firms to manage cyber risk and to report serious incidents
- Client confidentiality and privilege raise the stakes on every gap
- Clients, panels and insurers increasingly ask you to prove your security before they engage

How to use it

- Answer each question with evidence in mind, not good intentions
- Treat anything you cannot prove as a no
- Note the gaps, then use the roadmap near the end to decide what to tackle first

Control and visibility of your IT

Tests whether your IT is genuinely under control, or only assumed to be.

		Yes	No
1	Could you produce an accurate, current list of the systems, devices and cloud services that hold client matter files and case data, and say who owns each?	☐	☐
2	Does access follow need to know, so people reach only the matters their role requires, with confidential and privileged work walled off?	☐	☐
3	When a fee earner or staff member leaves or changes team, is their access changed the same day?	☐	☐
4	Are updates and security patches applied to a defined timescale (14 days) you could evidence?	☐	☐
5	Is a named person /persons accountable for IT and cybersecurity, with the authority to act, not only to advise?	☐	☐
6	If a key system or supplier failed tomorrow, would you quickly know which matters and deadlines would be affected?	☐	☐



Why this matters

You cannot demonstrate control of what you cannot see. In a firm built on confidentiality, clear ownership and current records are what turn a professional duty into evidence.

PROTECT

02

Data, identity and threat exposure

Looks past whether controls exist to whether they are switched on and working.

		Yes	No
1	Is multifactor authentication enabled, enforced and reviewed for every system that offers it, including email and your case management system?	☐	☐
2	Are the accounts and processes that can move client money or change bank details the most tightly controlled and monitored?	☐	☐
3	If a client or fee earner received a convincing email asking to change payment details, what would stop the money leaving?	☐	☐
4	Do you know where your most sensitive and privileged client data lives, and exactly who has access to it?	☐	☐
5	Are staff trained and tested on phishing and payment fraud, and is your firm protected against email impersonation?	☐	☐
6	Would your current controls alert you to suspicious activity, or would you hear it first from a client or the bank?	☐	☐



Why this matters

Law firms are a leading target for payment and email fraud, and a single conveyancing completion can move six figures. The question is never whether you own a control, but whether it is doing its job.

Continuity, recovery and resilience

Maps directly to the duties you owe clients and the regulator.

		Yes	No
1	Have you identified the main services that would harm clients most if they stopped working, such as access to matter files or the client account?	☐	☐
2	Do you know how long each could be down before you risk a missed court deadline or limitation date, and have you tested that you can stay within that time frame?	☐	☐
3	Have you actually restored client and matter data from a backup recently, rather than trusting that it would work?	☐	☐
4	Is at least one copy of your backup kept on a separate network or in a separate location, where a threat actor could not reach or delete it?	☐	☐
5	In the first hour of a serious incident, would everyone know their role, including who notifies clients, the SRA, the ICO and your insurer?	☐	☐
6	Could you show your regulator or insurer what happened, when, and how you responded?	☐	☐



Why this matters

A missed deadline, a lost file or misdirected client money is a regulatory and professional matter, not only an IT one. Untested recovery is where most firms fall short.

Turning trust into proof

Works whether you are certified already or only starting out.

		Yes	No
1	When a client, panel or insurer asks you to prove your security, can you point to an independent standard, or only describe your own efforts?	☐	☐
2	Do you know which assurances your professional indemnity insurer and client panels increasingly expect before they will work with you?	☐	☐
3	Does your security follow a recognised standard such as Cyber Essentials, Lexcel information management or ISO 27001?	☐	☐
4	If you already hold a certification, do you know exactly what it covers, and would you still pass if assessed today?	☐	☐
5	Has an independent party ever tested your defences, or has your security only been checked internally?	☐	☐
6	Do you treat certification as a live standard to keep up, rather than a badge earned once and filed away?	☐	☐



Why this matters

The SRA expects firms to prevent, detect and respond, and firms holding legal aid contracts must now hold Cyber Essentials. Certification turns your security from a claim into something clients, insurers and panels can verify.

Your resilience snapshot

What your answers tell you

Count the questions you could not answer yes to with evidence. You are not chasing a perfect score. You are finding the places where belief and evidence part company.

- 1** **Mostly yes.** A mature base. The task is to keep the evidence current and rehearsed.
- 2** **A mix of yes and no.** Real gaps worth closing before your next review or assessment.
- 3** **Mostly no.** Priority areas that leave the firm exposed and hard to defend to the SRA.

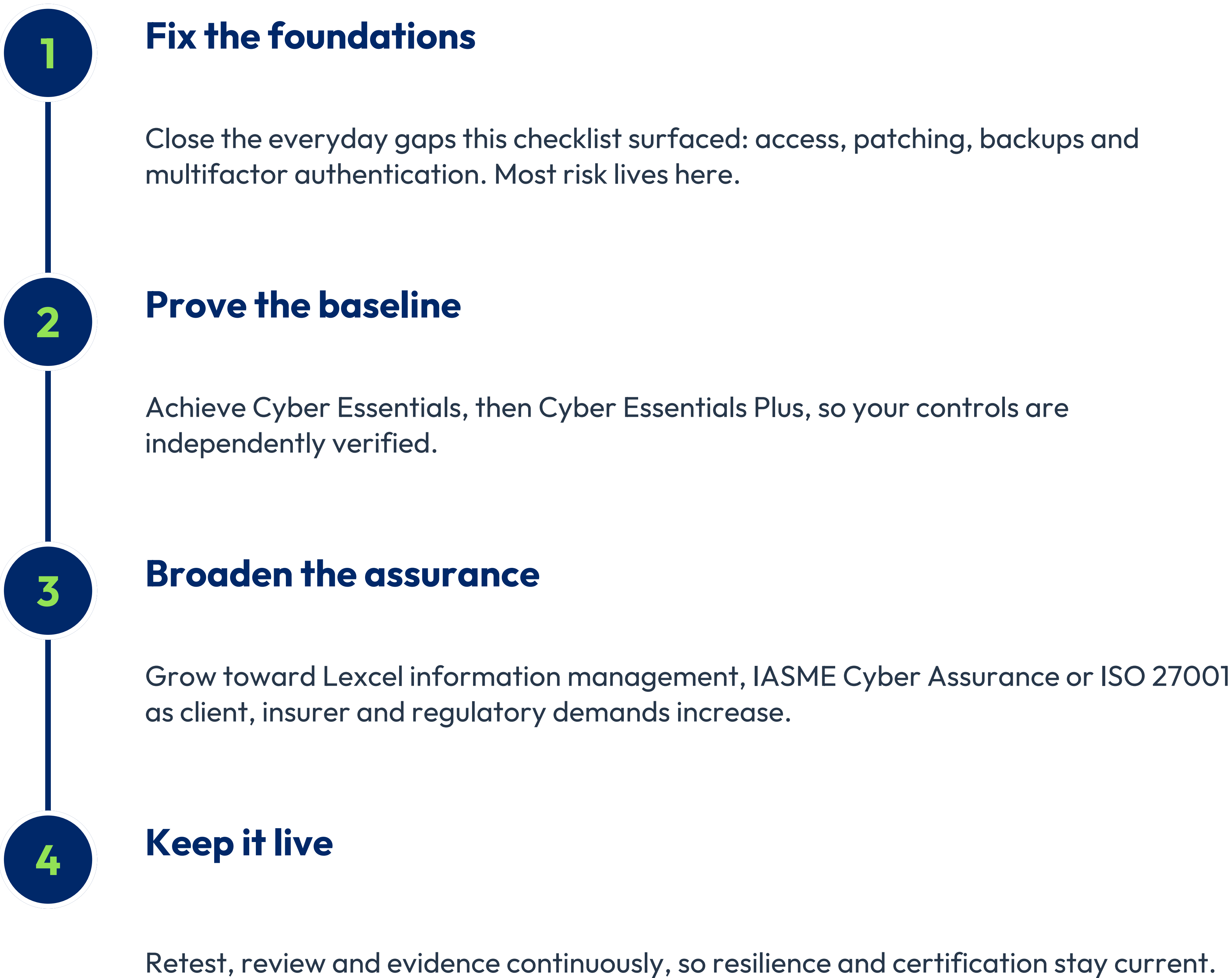
Treat these as red flags whatever your score

- You could not evidence how you would keep client matters running through disruption
- Your backups of client and matter data have not been restored and tested recently
- Multifactor authentication is not enabled on every service that offers it
- You rely on suppliers whose security you have never independently checked

A simple roadmap

Where to go from here

Wherever this checklist placed you, the path forward looks similar. Find your current stage and take the next step. Most firms sit between stages one and three, and steady progress matters more than a perfect score.

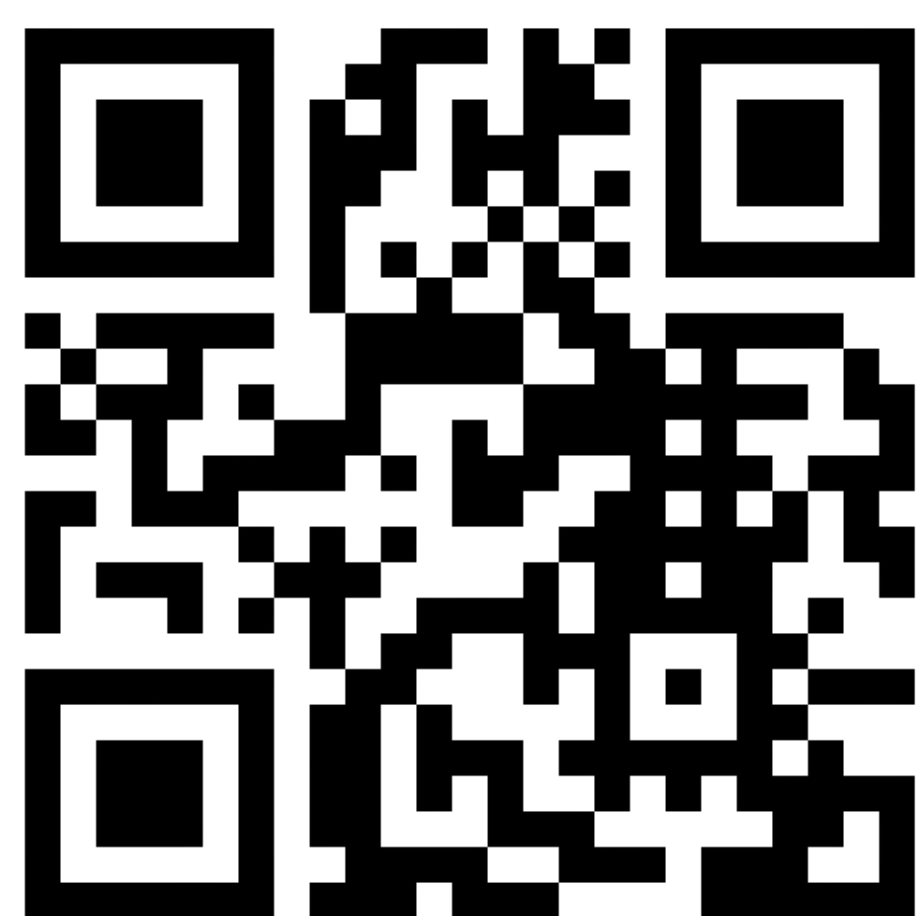


Next step

If you would like an independent view

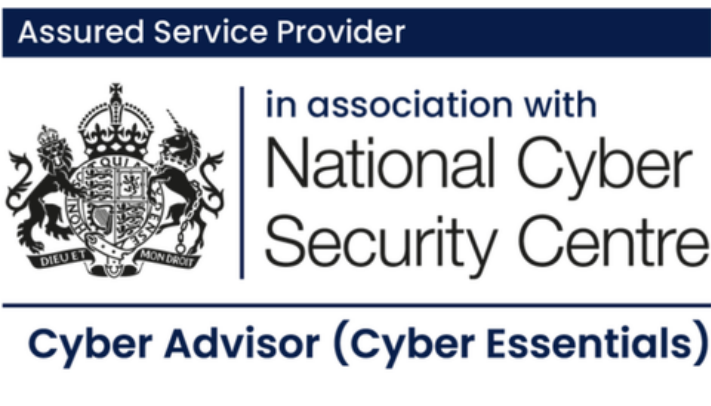
This checklist is a starting point, meant to help you see where you stand rather than to grade you. If you would like independent advice, you are welcome to request a consultation with our team.

How to get in touch



Email
info@complus-it.com

Address
107-111 Fleet St, London EC4A 2AB



This checklist reflects UK requirements in force as at August 2026, including SRA expectations, UK GDPR breach reporting and the 2026 Cyber Essentials requirements. It is general guidance and not regulatory or legal advice.