CICADA | RESOURCES

RESPONSE | 45 MIN | WORKING KNOWLEDGE | UPDATED NOVEMBER 2026

Know which suppliers could take you down

Your IT provider, accountant, payroll bureau and booking platform may hold the keys to your business.

The short version

- ✓ List suppliers by what they can access, not what they sell.
- ✓ Ask every critical supplier whether they use MFA .
- ✓ Know how to reach each one out of hours.
- ✓ Remove access the moment a contract ends.

Build the list

For each supplier: what they can access, who owns the relationship, how to reach them in an incident, contract end date, and whether they hold customer or financial data. Start with IT, accounting, payroll, banking, payment processing, website and email.

Include freelancers and contractors. The person who built your website may still have admin access years later.

Ask three questions

01 Do you use MFA on the accounts that access our systems?

02 Who at your company can see our data, and how do you remove access when someone leaves?

03 How would you tell us about a breach, and how quickly?

You don't need a 50-page questionnaire for a five-person business. You need to know whether the basics exist and whether the answer is credible.

Manage the relationship

Review access annually. Remove it when the contract ends. Don't let a supplier use a shared login with a password sent by email. If a critical supplier can't answer basic security questions, consider whether the convenience is worth the concentration risk.

> **CONCENTRATION RISK**
>
> If one supplier going down would stop you trading, you need a fallback, or at least a tested way to reach them and a copy of your data.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

Action checklist

- [ ] Critical suppliers listed with access
- [ ] Incident contacts verified
- [ ] MFA question asked and recorded
- [ ] Contract end dates tracked
- [ ] Access removed at offboarding
- [ ] Fallback plan for single points of failure

0 of 6 done