

The Cyber Security Vendor Red Flags Handbook

How to Spot Risk Before You Sign Anything

Executive Summary

This handbook helps SMEs identify early warning signs that a vendor may not be suitable, reliable, or safe to work with.

1. Commercial Red Flags

- Vague pricing
- Hidden onboarding fees
- No written SLAs
- No liability clarity

2. Technical Red Flags

- No integration documentation
- No architecture diagrams
- No API references
- No security testing evidence

3. Compliance Red Flags

- No DPA
- No breach notification process
- No audit trail
- No certification evidence

4. Support Red Flags

- Outsourced support with no transparency
- No guaranteed response times
- No escalation path

5. Behavioural Red Flags

- Over-promising
- Avoiding direct questions
- Pressuring for quick decisions
- Refusing to provide references

Conclusion

Spotting red flags early saves SMEs time, money, and risk.