Vendor Cybersecurity Audit Checklist for SMBs

A practical tool to evaluate your third-party vendors before onboarding.

Category	Low Risk	Medium Risk	High Risk
Data Sensitivity	✅	⚠️	❌
Compliance Level	✅	⚠️	❌
Incident History	✅	⚠️	❌

Pro Tip: Assign scores (Yes = 1, No = 0). Vendors scoring below 70% should be reviewed carefully.

Checklist Sections

1. Basic Vendor Information

- ☐ Does the vendor have a documented security policy?
- ☐ Is there a dedicated security officer or team?
- ☐ How long has the vendor been operating in the market?

2. Data Protection & Privacy

- ☐ Does the vendor encrypt data at rest and in transit?
- ☐ Do they support role-based access controls?
- ☐ Do they comply with relevant data privacy laws (GDPR, HIPAA, CCPA)?

3. Infrastructure & Application Security

- [ ] Are systems regularly patched and updated?
- [ ] Are APIs tested for vulnerabilities (OWASP Top 10)?
- [ ] Do they perform regular penetration tests or third-party audits?

4. Incident Response & Monitoring

- [ ] Does the vendor have a breach notification process?
- [ ] Do they offer audit logs or monitoring dashboards for clients?
- [ ] Have they had a security incident in the last 24 months?

5. Compliance & Certifications

- [ ] SOC 2 / ISO 27001 / PCI DSS certified?
- [ ] Do they provide compliance reports upon request?
- [ ] Are subcontractors also compliant?