IronRoot
Risk Consultants

Are You Audit-Ready?

Small Business Security Self-Assessment Quiz

Score each question honestly based on your current state -- not where you plan to be. Add up your points to see your overall security posture rating. Maximum score: 60 points.

Section A: Governance & Policies

1. We have a written information security policy that has been reviewed in the last 12 months.

[ ] **(4 pts)** Yes, reviewed and up to date
[ ] **(2 pts)** Yes, but not recently reviewed
[ ] **(0 pts)** No written policy

Question 1 Score: _____ / 4

2. All employees have received cybersecurity awareness training in the last 12 months.

[ ] **(4 pts)** Yes, formal annual training
[ ] **(2 pts)** Ad hoc or informal training only
[ ] **(0 pts)** No training program

Question 2 Score: _____ / 4

3. We have a written incident response plan that staff know how to use.

[ ] **(4 pts)** Yes, tested in last 12 months
[ ] **(2 pts)** Written plan, never tested
[ ] **(0 pts)** No written plan

Question 3 Score: _____ / 4

Section B: Access & Identity

4. Multi-factor authentication (MFA) is enforced on all business email accounts.

[ ] **(4 pts)** Yes, enforced for all users
[ ] **(2 pts)** Available but not enforced
[ ] **(0 pts)** Not enabled

Question 4 Score: _____ / 4

5. We have a formal offboarding process that removes all system access on the employee's last day.

[ ] **(4 pts)** Yes, documented and consistently followed
[ ] **(2 pts)** Informal process, sometimes missed
[ ] **(0 pts)** No formal process

Question 5 Score: _____ / 4

6. We conduct periodic access reviews to verify that only current staff have active accounts.

[ ] **(4 pts)** Yes, at least quarterly
[ ] **(2 pts)** Ad hoc, no schedule
[ ] **(0 pts)** Never reviewed

Question 6 Score: _____ / 4

Section C: Data Protection & Backups

7. We have documented what sensitive data we hold and where it is stored.

[ ] **(4 pts)** Yes, current data inventory
[ ] **(2 pts)** Partial or outdated inventory
[ ] **(0 pts)** No data inventory

Question 7 Score: _____ / 4

8. Our backups have been tested by performing a successful restore in the last 12 months.

[ ] **(4 pts)** Yes, restore test completed and documented
[ ] **(2 pts)** Backup exists but never tested
[ ] **(0 pts)** No regular backup

Question 8 Score: _____ / 4

9. Sensitive data is encrypted both at rest and in transit.

[ ] **(4 pts)** Yes, encryption enforced across all systems
[ ] **(2 pts)** Partial encryption
[ ] **(0 pts)** No encryption in use

Question 9 Score: _____ / 4

Section D: Incident Response

10. We have identified who is responsible for declaring a security incident and initiating response.

[ ] **(4 pts)** Yes, defined with documented contacts
[ ] **(2 pts)** Informally understood
[ ] **(0 pts)** Not defined

Question 10 Score: _____ / 4

11. We know which legal, regulatory, or contractual breach notification obligations apply to us.

[ ] **(4 pts)** Yes, documented with timelines
[ ] **(2 pts)** Aware but not documented
[ ] **(0 pts)** Not aware of obligations

Question 11 Score: _____ / 4

12. We have cyber liability insurance that specifically covers data breach and ransomware costs.

[ ] **(4 pts)** Yes, standalone cyber policy
[ ] **(2 pts)** Believe it may be covered under existing policy
[ ] **(0 pts)** No cyber coverage

Question 12 Score: _____ / 4

Section E: Vendor & Third-Party Risk

13. We maintain an inventory of all vendors with access to our systems or data.

[ ] **(4 pts)** Yes, current and complete
[ ] **(2 pts)** Partial list, not maintained
[ ] **(0 pts)** No vendor inventory

Question 13 Score: _____ / 4

14. Our vendor contracts include security requirements and breach notification clauses.

[ ] **(4 pts)** Yes, in all contracts
[ ] **(2 pts)** Some contracts, not all
[ ] **(0 pts)** No security requirements in contracts

Question 14 Score: _____ / 4

15. We have reviewed the security posture of our highest-risk vendors in the last 12 months.

[ ] **(4 pts)** Yes, formal review or SOC 2 review
[ ] **(2 pts)** Informal review
[ ] **(0 pts)** No vendor security review

Question 15 Score: _____ / 4

Score Tally

Section	Questions	Max	Your Score
A: Governance & Policies	3	12	_____
B: Access & Identity	3	12	_____
C: Data Protection & Backups	3	12	_____
D: Incident Response	3	12	_____
E: Vendor & Third-Party Risk	3	12	_____
TOTAL	**15**	**60**	_____

How to Interpret Your Score

Score	Rating	What It Means
55-60	**STRONG**	Your security posture is well-developed. Focus on continuous improvement and annual reviews.
45-54	**DEVELOPING**	Good foundation in place with some gaps to address. Prioritize untested controls.
35-44	**MODERATE**	Significant gaps present. Several controls need immediate attention to reduce exposure.

20-34	**HIGH RISK**	Multiple critical gaps identified. Engage a security advisor and address highest-risk areas first.
0-19	**CRITICAL**	Immediate action required. Your organization has significant exposure across multiple risk areas.

Ready to Close Your Gaps?

IronRoot Risk Consultants helps small businesses translate quiz results into an action plan.

chris@ironrootrisk.com | ironrootrisk.com