

SMALL-BUSINESS CHECKLIST · 01 / 02

Know the gaps before you buy another tool.

This is a conversation starter for business owners. Mark **yes / no / unknown**, write down who owns the answer, and select the next action. An “unknown” is a useful finding—not a failing grade.

Do not write passwords, recovery codes, payment information, customer records or incident evidence on a shared copy. This worksheet is not a risk assessment, compliance audit or security certification.

1 Know what matters

- ☐ Can someone name the systems and data the business depends on most?
- ☐ Is there an owner for security decisions and priority spending?
- ☐ Is there a current list of devices, key apps, admin accounts and outside providers?

2 Protect access

- ☐ Is multi-factor authentication used for important accounts where supported?
- ☐ Are new accounts approved and departing users removed through a repeatable process?
- ☐ Do staff know how to report suspicious messages or account activity?

3 Maintain systems

- ☐ Are devices and software updated through a defined routine?
- ☐ Are unsupported systems identified and assigned a decision?
- ☐ Does someone review vendor access and changes?

4 Prepare to recover

- ☐ Does an owner know what is backed up—and what is not?
- ☐ Has a restore been tested for an important workflow and recorded?
- ☐ Is there a first-response path if a security incident is suspected?

Which answer surprised you most?

Question / owner / what you need to verify

Built as original WOLFTRAXX SYSTEMS copy using small-business risk themes from the NIST Cybersecurity Framework 2.0 Small Business Quick Start Guide and CISA small-business resources. It does not reproduce a competitor checklist or imply agency endorsement.

SMALL-BUSINESS CHECKLIST · 02 / 02

Give the next three actions an owner.

A useful first plan balances business ownership, a practical protection gap, and the ability to respond or recover. Choose actions you can verify, not just another product name.

Priority	Next action and evidence	Owner	Target date
1 · Ownership gap	Decision / policy / vendor responsibility		
2 · Protection gap	Access / device / update control		
3 · Recovery gap	Restore / contact / response test		

Questions worth asking your technology provider

Scope & evidence

- ☐ Which systems and people are in scope?
- ☐ What will be checked or changed—and what will not?
- ☐ What evidence will we receive when the work is done?

Responsibility

- ☐ Who makes the business decision?
- ☐ Who performs the work and who reviews it?
- ☐ What is the agreed path if an issue is found later?

Open questions

Questions to bring to a scoped conversation

Make the next step specific.

WOLFTRAXX SYSTEMS can discuss a scoped security conversation for your business. Start at wolftraxxsystems.com/contact/ or call **888.758.8577**. Do not send sensitive details in an initial inquiry.

Source themes: NIST CSF 2.0 Small Business Quick Start Guide, nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0; CISA small-business resources, cisa.gov/small-and-medium-sized-business-resources (reviewed 2026-10-03). Read the online version at wolftraxxsystems.com/small-business-security-readiness/. Any assessment or ongoing service requires separately agreed scope.