berruit

FREE RESOURCE · 2026

Small business cybersecurity checklist

24 controls in 6 areas to see where your company's security stands and what to fix first. Check, add up your score and prioritize.

24	6	5 min
security controls	areas assessed	to complete

BEFORE YOU START

How to use this checklist

It is a guide based on general best practices. Answer honestly and, if you can, do it with whoever manages your systems.

1. **Mark one answer per control.**
   Yes if it is in place and working; Partial if it exists but is incomplete; No if it does not exist or you do not know.

2. **Add up the points for each area.**
   Yes is worth 2 points, Partial 1 point and No 0 points. Each area adds up to a maximum of 8 points.

3. **Find your level and prioritize.**
   Copy the totals to the score sheet, identify the areas with the fewest points and fill in the action plan.

HOW TO READ YOUR TOTAL SCORE (OUT OF 48 POINTS)

0–39%	**High risk**	Your company has basic gaps an attacker can exploit. Make them a priority as soon as possible.
40–64%	**Incomplete baseline**	You have important controls, but some areas are not covered. Closing those gaps lowers your risk significantly.
65–84%	**Good level, with gaps**	Most controls are in place. Review the lowest-scoring areas to complete your protection.
85–100%	**Strong level**	Your company covers almost every control. Keep them current and validate them with an external review.

This checklist is not an audit and does not certify compliance with any standard. It is a starting point for a conversation with your team or a specialist.

MARK YOUR ANSWERS

01 Access and identities

Who gets into your systems, with which credentials and how far they can go.

1	**We use multi-factor authentication (MFA) on email and on every remote access.** A stolen password is not enough to get in if there is a second verification factor.	☐ Yes	☐ Partial	☐ No
2	**Each person has their own user account: we do not share accounts or passwords.** Without individual accounts there is no way to know who did what.	☐ Yes	☐ Partial	☐ No
3	**Administrator rights are limited to those who need them and are reviewed at least once a year.** Fewer privileged accounts reduce what an attacker can take over.	☐ Yes	☐ Partial	☐ No
4	**When someone leaves the company, we disable their access the same day.** Former employees' accounts that stay active are a forgotten door.	☐ Yes	☐ Partial	☐ No

Area points: _____ / 8

02 Computers and servers

The computers, phones and servers where your information lives.

5	**All computers and servers have managed, up-to-date antivirus or EDR.** Antivirus that is outdated or has no central console leaves devices unprotected without anyone noticing.	☐ Yes	☐ Partial	☐ No
6	**Windows and critical applications are updated through a defined patching routine.** Many attacks exploit vulnerabilities that already have a patch available.	☐ Yes	☐ Partial	☐ No
7	**Laptops and phones with company information have encryption and a screen lock.** If an encrypted device is lost, the information is not exposed.	☐ Yes	☐ Partial	☐ No
8	**We keep an up-to-date inventory of hardware and software, with current licenses.** You cannot protect what you do not know exists.	☐ Yes	☐ Partial	☐ No

Area points: _____ / 8

MARK YOUR ANSWERS

03 Network and remote access

The front door of your network and how people connect from outside.

9	**A firewall protects the network, and its rules and updates are reviewed periodically.** A firewall that is installed but not maintained stops protecting over time.	☐ Yes	☐ Partial	☐ No
10	**Guest Wi-Fi is separated from the company's internal network.** That way an outside device cannot reach your servers or shared folders.	☐ Yes	☐ Partial	☐ No
11	**Employees and vendors connect remotely through a VPN or another secure method with MFA.** Uncontrolled remote access is one of the entry points attackers use most.	☐ Yes	☐ Partial	☐ No
12	**Someone reviews alerts and logs from the firewall and critical systems.** Without monitoring, an incident can go unnoticed for weeks.	☐ Yes	☐ Partial	☐ No

Area points: _____ / 8

04 Backup and continuity

What happens to your operation if you lose data or systems go down.

13	**Backups of critical information run automatically.** Manual backups depend on someone remembering to make them.	☐ Yes	☐ Partial	☐ No
14	**We keep at least one copy outside the main network (cloud or immutable storage).** Ransomware also encrypts the backups it can reach on the network.	☐ Yes	☐ Partial	☐ No
15	**We test restoring a backup at least once a year.** A backup that has never been restored is an assumption, not a guarantee.	☐ Yes	☐ Partial	☐ No
16	**We have written down which systems are critical and how long we can be without them.** Without that definition there is no way to prioritize recovery when something fails.	☐ Yes	☐ Partial	☐ No

Area points: _____ / 8

MARK YOUR ANSWERS

05 People and data

The human factor and control over sensitive information.

17	**The team receives training or phishing simulations at least once a year.** Many incidents start with a fake email that someone opens.	☐ Yes	☐ Partial	☐ No
18	**There is an acceptable use policy for devices, email and passwords that everyone knows.** Rules that are not written down and communicated cannot be enforced.	☐ Yes	☐ Partial	☐ No
19	**We know where personal and sensitive data lives and who can access it.** It is the starting point for protecting it and meeting your privacy obligations.	☐ Yes	☐ Partial	☐ No
20	**We control sensitive information leaving the company by USB, email or cloud.** Many data leaks come from internal mistakes, not external attacks.	☐ Yes	☐ Partial	☐ No

Area points: _____ / 8

06 Response, support and compliance

How you react when something goes wrong and what backs you up.

21	**There is a clear procedure to report an incident and everyone knows whom to call.** In an incident, every hour without an organized response increases the damage.	☐ Yes	☐ Partial	☐ No
22	**We have IT or security support with defined response times.** An agreed response time avoids depending on someone's goodwill.	☐ Yes	☐ Partial	☐ No
23	**After an incident we review what failed and fix the cause.** Without that review, the same problem comes back.	☐ Yes	☐ Partial	☐ No
24	**We know which laws and contracts require us to protect data, and we have a written privacy and security policy.** Obligations depend on your industry, your customers and the states and countries where you operate.	☐ Yes	☐ Partial	☐ No

Area points: _____ / 8

RESULTS

Score sheet

AREA	POINTS	MAXIMUM	%
01 Access and identities		8	
02 Computers and servers		8	
03 Network and remote access		8	
04 Backup and continuity		8	
05 People and data		8	
06 Response, support and compliance		8	
Total		**48**	

Area % = points ÷ 8 × 100. Total % = points ÷ 48 × 100. My level: _____

Action plan

Start with the lowest-scoring areas and the controls you marked as No.

THIS WEEK	THIS MONTH	THIS QUARTER

berruit

NEXT STEP

Would you like us to review your result with you?

A Berruit consultant reviews your infrastructure, access, backups and support, and tells you what to improve first. The initial assessment is free.

✓ Free assessment ✓ No commitment ✓ A reply from a real consultant

---

WEB
berruit.com/en

WHATSAPP AND PHONE
+1 305 404 5212

EMAIL
info@berruit.com

LOCATION
Berruit LLC
Fort Walton Beach, FL

A guide based on general cybersecurity best practices. It is not an audit and does not certify compliance with any standard or law.