MORE POWER TECHNOLOGY GROUP

C H E C K L I S T

Lean IT Security Visibility Checklist

20 questions for a first review of your technology visibility and responsibilities.

Complete this with whoever handles your technology. Mark **Yes** when you can support the answer, **No** when the arrangement is missing, and **Not sure** when it needs checking. Allow about 20 minutes for a first pass, then follow up on missing information. Do not enter passwords or sensitive system details.

Organization _____ **Completed with** _____ **Date** _____

1. DO YOU KNOW WHAT YOU HAVE?

Include remote work and equipment bought or replaced outside the usual IT process.

Question	Yes	No	Not sure
1. Do you have a current inventory of devices connected to your network or used to access your data?	☐	☐	☐
2. Has someone reviewed that inventory within the last 12 months and checked subsequent changes?	☐	☐	☐
3. Do you know which work devices leave the building or are used remotely?	☐	☐	☐
4. Would your IT contact know if a department bought and connected a new device?	☐	☐	☐

2. DO YOU KNOW WHAT IS PROTECTED?

Check current status, not just the original deployment. Record any unsupported devices or exceptions.

Question	Yes	No	Not sure
5. Is endpoint security installed on the workstations and servers that require it?	☐	☐	☐
6. Do you know the actual coverage percentage and how it was calculated?	☐	☐	☐
7. Does someone verify that security agents are running, current, and reporting?	☐	☐	☐
8. Do you know which devices, if any, lack endpoint protection?	☐	☐	☐

3. DO YOU KNOW WHAT IS HAPPENING?

Device, email, and account activity may come from different sources. Confirm which are included.

Question	Yes	No	Not sure
9. Are security events being logged on the systems and services you rely on?	☐	☐	☐
10. Do you know how long those logs remain available?	☐	☐	☐
11. Does someone review security alerts on an agreed schedule?	☐	☐	☐
12. Would a sign-in from an unexpected country be identified and reviewed?	☐	☐	☐

4. DO YOU KNOW WHO OWNS THE NEXT ACTION?

A named owner needs time, authority, and support. Alert review and incident response are different responsibilities.

Question	Yes	No	Not sure
13. Is there a named person or provider contact for alert review, with backup coverage?	☐	☐	☐
14. Is alert review a documented job or service responsibility?	☐	☐	☐
15. Do you know what your monitoring provider is contracted to do when a problem is found?	☐	☐	☐
16. Have you reviewed the exclusions in your monitoring or IT agreement?	☐	☐	☐

5. COULD YOU FIND THESE ANSWERS DURING AN INCIDENT?

Check that essential contacts and plans are accessible if your normal systems are unavailable.

Question	Yes	No	Not sure
17. Do you know when backups were last tested by restoring data or a system?	☐	☐	☐
18. Can you reach your cyber-insurance claims contact without using your network?	☐	☐	☐
19. Do you know who to contact first if you suspect an incident tonight?	☐	☐	☐
20. Is a written incident plan accessible to the people who may need it after hours?	☐	☐	☐

REVIEW YOUR ANSWERS

Count: Yes _____ **No** _____ **Not sure** _____

Total: 20.

Use the count to organize follow-up, not to grade your security. These are editorial planning bands, not validated risk levels, compliance findings, or peer benchmarks.

16–20 Yes: review each remaining gap and confirm the evidence behind your answers. **10–15 Yes:** group the open questions by section and assign follow-up. **0–9 Yes:** start by establishing inventory and coverage, while assigning responsibility for alert review and action.

Regardless of the total: follow up on any **No** or **Not sure** in section 4. Confirm who reviews a finding, who approves action, and who performs the work. A high count of Yes answers does not close an ownership gap.

CHOOSE THE NEXT USEFUL RESOURCE

For responsibilities, read IT Monitoring vs. Managed IT Services. For coverage, use the endpoint monitoring guide. For incident preparation, use What to Do If You Suspect a Cyber Breach.

MPTG's Network Self-Assessment collects contact and environment details for follow-up from MPTG. To discuss whether monitoring fits, bring this checklist to a Sentry Fit Review.

Next action _____ **Owner** _____ **Review date** _____

REFERENCE

NIST SP 1300: Small Business Quick-Start Guide, February 2024, provides related guidance on inventory, protection, monitoring, and response. This checklist is MPTG planning content, not a NIST assessment.