



Professional IoT Security Readiness Audit Checklist

Home and Small Business Connected Device Self-Assessment

Score each item:

- **Yes = 2 points**
 - **Partially = 1 point**
 - **No = 0 points**
-

Visibility & Inventory

- We maintain a current list of all internet-connected smart devices.
- Each device has a documented owner or responsible user.
- Unused or old connected devices are removed from the environment.

Authentication

- Default passwords have been changed on all smart devices.
- Mobile companion apps use strong unique passwords.
- MFA is enabled on vendor cloud accounts where available.

Firmware & Vendor Support

- Firmware updates are checked regularly.
- Unsupported or discontinued devices are being phased out.
- Vendor mobile apps are still actively maintained.

Network Security

- Wi-Fi router admin credentials have been changed from default.
- Router firmware is current.
- Guest or low-trust devices are separated where possible.

Privacy & Cloud Awareness

- Camera/microphone devices have reviewed sharing permissions.
- Cloud retention and linked users are periodically checked.
- Sensitive devices are not casually shared across many users.

Business IoT Governance

- Office cameras, POS tools, printers, and smart controls have assigned oversight.
- Non-IT departments notify management before adding connected hardware.
- Connected operational devices are included in cyber discussions.

Incident Readiness

- We know how to disconnect or isolate a suspected compromised device quickly.
- Linked app accounts can be changed rapidly if compromise is suspected.
- Basic logs/screenshots are preserved before replacing hardware.

Ongoing Discipline

- Quarterly IoT reviews are performed.
- Family members or employees receive smart-device security guidance.

SCORING RESULTS

38–46 Points — STRONG MATURITY

Your home or business demonstrates strong practical awareness of connected-device security and reduced hidden IoT exposure.

20–37 Points — MODERATE EXPOSURE

Important protections exist, but forgotten devices, weak app controls, or network trust gaps may still create preventable risk.

0–19 Points — HIGH VULNERABILITY

Your connected environment likely contains multiple silent IoT weaknesses that could expose privacy, network safety, or operational continuity.