Year-End IT Checkup Checklist for Small Businesses (2026 Edition)

Use this checklist to evaluate your current setup and identify where your business may be exposed.

Year-End IT Checkup Checklist

1. System and Software Updates

□ Operating systems (Windows, macOS, servers) are fully updated
□ Third-party apps (browsers, QuickBooks, Adobe, etc.) are current
□ You have visibility into which devices are missing patches
□ Domains, SSL certificates, and licenses are not near expiration

Why this matters:
Unpatched systems are one of the most common entry points for security issues and downtime.

2. Security and Password Protection

□ Antivirus or endpoint protection is active and updated
□ MFA is enabled for all users and critical systems
□ Password policies are enforced (no reuse, strong passwords)
□ Password manager is used across the team

Why this matters:
Most breaches begin with compromised credentials—not advanced attacks.

3. Backup and Recovery Readiness

- ☐ Backups are running successfully
- ☐ Backup logs are reviewed regularly
- ☐ Test restores have been performed
- ☐ Backups are stored securely and offsite
- ☐ Recovery time expectations are understood

Why this matters:
Backups only protect your business if they are verified and recoverable.

4. Hardware and Performance Health

- ☐ Devices are cleaned and maintained (dust, overheating, etc.)
- ☐ Hardware age and warranty status are tracked
- ☐ Network devices are updated and functioning properly
- ☐ Wi-Fi coverage and performance meet business needs

Why this matters:
Performance issues often signal aging hardware or hidden failures.

5. Data Protection and Compliance

- ☐ Data retention and disposal policies are defined
- ☐ Access to sensitive data is restricted appropriately
- ☐ Data is encrypted where required
- ☐ Compliance requirements (HIPAA, PCI, etc.) are reviewed

Why this matters:
Data mismanagement creates both security risk and compliance exposure.

6. Vendor and Access Review

- ☐ Third-party vendors with access to systems or data are identified
- ☐ Vendor access is limited and reviewed
- ☐ Unused accounts and permissions are removed
- ☐ SaaS and cloud tools are accounted for

Why this matters:
Vendors and apps often create hidden risk if not reviewed regularly.

7. Incident and Risk Awareness

- ☐ Recent IT issues or outages have been reviewed
- ☐ Patterns or recurring problems are identified

◻ Employees know how to report suspicious activity
◻ Incident response plan exists and is accessible

Why this matters:
Past issues often reveal future risks.

8. Planning for the New Year

◻ Upcoming renewals (licenses, domains, warranties) are tracked
◻ Budget includes hardware refreshes and upgrades
◻ IT priorities are defined for the next year
◻ Growth plans (new hires, expansion, systems) are considered

Why this matters:
IT should support where your business is going—not just maintain where it is.

What a Healthy IT Environment Looks Like

Systems are updated and monitored
Security controls are active and enforced
Backups are verified and recoverable
Hardware is reliable and planned for
Risks are known—not guessed

Quick Rule of Thumb

If you're unsure about multiple items on this checklist, your IT environment likely has hidden risks.