SAGE SOLUTIONS

10-Point IT Health Checklist

A self-scoring assessment for small and mid-sized businesses across NY and NJ.

How to use this checklist

For each of the 10 items, score yourself 1–5. Total your score at the end. The interpretation key is on the final page. There are no trick questions — this is the same checklist we use on first-call assessments for new clients.

Score	What it means
1	Not in place, or we don't know
2	Partially in place, inconsistent
3	In place, but not verified or documented
4	In place, documented, periodically tested
5	In place, documented, continuously monitored

01 Backups — and recovery has actually been tested

THE QUESTION

When was the last time you successfully restored a representative file, mailbox, and full server from backup, in an isolated environment, with a documented result?

WHAT GOOD LOOKS LIKE

- Image-based backup of every server and critical workstation
- Off-site replication to immutable storage (an attacker who fully owns your network cannot delete the backup chain)
- Backups verified daily; recovery exercised at least quarterly with documented results
- Documented Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

COMMON FAILURE MODES

Backups have been "running" for years but have never been restored. Backups are on a USB drive in the same building. Backups are reachable by an attacker who compromises the domain.

Your score: ___ / 5

02 Multi-factor authentication on every business-critical system

THE QUESTION

Is MFA enforced on email, line-of-business apps, VPN, file sharing, financial systems, and any system that touches customer or employee data?

WHAT GOOD LOOKS LIKE

- MFA enforced (not just available) on every critical system
- Phishing-resistant MFA where possible (FIDO2 keys, app-based push, certificate-based)
- Conditional access based on device trust, location, and risk signals
- MFA reset process documented and secure

COMMON FAILURE MODES

MFA on email but not on VPN. MFA available but not enforced. SMS-only MFA on critical systems. No process for MFA recovery.

Your score: ___ / 5

03 Endpoint Detection and Response (EDR) on every endpoint

THE QUESTION

Is there an EDR product running on every workstation and server, with a SOC monitoring the alerts?

WHAT GOOD LOOKS LIKE

- EDR (CrowdStrike, SentinelOne, Defender for Endpoint, Huntress) on every endpoint
- 24/7 monitoring by an internal team or an MDR provider
- Documented response procedures
- Periodic verification that EDR is healthy on every device

COMMON FAILURE MODES

Free or consumer-grade antivirus instead of EDR. EDR installed but no one monitors alerts. EDR missing on a few "edge case" machines.

Your score: ___ / 5

04 Email security and phishing resilience

THE QUESTION

Are inbound emails filtered for phishing, malware, and impersonation, and are users trained to recognize what gets through?

WHAT GOOD LOOKS LIKE

- Email gateway with anti-phishing (Proofpoint, Mimecast, M365 Defender, Avanan)
- DMARC, SPF, and DKIM properly configured for outbound
- Phishing simulations run regularly, with click-rate tracking
- Annual security awareness training for every user
- Reporting button for users to flag suspicious messages

COMMON FAILURE MODES

Default M365 protection only. No DMARC enforcement. Phishing training is "we sent an email about it once."

Your score: ___ / 5

05 Patch management

THE QUESTION

Are operating systems, third-party applications, and firmware patched on a documented schedule?

WHAT GOOD LOOKS LIKE

- Automated OS patching for Windows, macOS, and Linux endpoints
- Third-party application patching (browsers, Office, Adobe, Java)
- Firmware patching for firewalls, switches, access points
- Patching cycle documented (critical patches within 7 days, others within 30)
- Reporting on patch compliance

COMMON FAILURE MODES

Windows updates left to user discretion. Third-party apps never updated. Firewall firmware untouched for years.

Your score: ___ / 5

06 Network segmentation

THE QUESTION

Are guest Wi-Fi, IoT devices, POS systems, and PHI/cardholder-data systems on separate network segments from your main user network?

WHAT GOOD LOOKS LIKE

- Separate VLANs: user, guest, IoT/printers, POS, PHI/payment systems
- Firewall rules that enforce segmentation
- Documented network diagram

COMMON FAILURE MODES

Flat network. Guest Wi-Fi shares the same VLAN as the POS. IoT on the user network. No diagram exists.

Your score: ___ / 5

07 Privileged access management

THE QUESTION

Are administrator accounts separate from daily-use accounts, with documented controls?

WHAT GOOD LOOKS LIKE

- Domain admin accounts used only for admin work
- No shared "admin" accounts
- Service accounts inventoried and rotated
- Just-in-time admin access where possible
- MFA enforced on every admin account

COMMON FAILURE MODES

IT staff use domain admin for daily email. Shared admin password known by multiple people. Service account passwords last rotated five years ago.

Your score: ___ / 5

08 Cyber insurance and breach response readiness

THE QUESTION

Do you have cyber insurance with a reputable carrier, a known incident response retainer, and a documented response plan?

WHAT GOOD LOOKS LIKE

- Cyber insurance policy reviewed annually
- Breach coach / IR retainer documented
- Incident response runbook with names, phone numbers, and decision authority
- Annual tabletop exercise

COMMON FAILURE MODES

No cyber insurance. Policy hasn't been reviewed since it was bought. No one knows who to call when something happens.

Your score: ___ / 5

09 Vendor and access offboarding

THE QUESTION

When an employee or vendor leaves, how fast and how completely is their access revoked across every system?

WHAT GOOD LOOKS LIKE

- Documented offboarding checklist for every system the person had access to
- Centralized identity (Entra ID, Okta, Google Workspace)
- Quarterly access reviews
- Vendor access tracked and reviewed

COMMON FAILURE MODES

Account disabled in M365 but still active in 12 SaaS apps. Departed employees still have VPN access months later.

Your score: ___ / 5

10 Documentation

THE QUESTION

If your IT person disappeared tomorrow, could a new IT person take over with what is documented?

WHAT GOOD LOOKS LIKE

- Network diagram, current
- Inventory of all hardware, software, licenses
- Documented passwords / secrets in an encrypted vault
- Vendor contact list with account numbers
- Standard operating procedures for routine tasks

COMMON FAILURE MODES

Documentation lives in one person's head. Passwords in a spreadsheet. No network diagram or one years out of date.

Your score: ___ / 5

YOUR RESULTS

Total your score

Add up your 10 scores. Total: ____ / 50

Score	What it means
45 – 50	Strong posture. Continue periodic review.
35 – 44	Functional with material gaps. Prioritize the lowest-scoring areas.
25 – 34	Significant risk. A serious incident would be hard to recover from.
Under 25	High risk. Address foundational gaps this quarter.

If your score is below 35

The highest-leverage actions are usually:

- Test your backups — actually restore something, today.
- Enforce MFA on every business-critical system.
- Deploy EDR if you don't have it.
- Document an incident response plan with phone numbers.
- Verify cyber insurance is current and adequate.

Want a free 30-minute review with a senior engineer?

Book at **sagesolutionsllc.net/contact** or call **(646) 886-7604**. No deck. No high-pressure sales. A written assessment in 48 hours.

This checklist is general guidance for NY/NJ small and mid-sized businesses. Specific compliance, regulatory, or insurance requirements may vary. © Sage Solutions LLC.