



15 Things Every Business Should Know About Its IT Infrastructure

A practical self-assessment checklist for business owners, managers and decision-makers.

Before you spend more money on IT, understand what you already have, what is working, what is exposed, and what needs to be improved.

GA Tech
IT Infrastructure Documentation & Audit
Document. Assess. Optimize. Plan.

How to Use This Guide

This checklist is designed to give you a quick picture of your organization's IT maturity. It is not a replacement for a professional technical audit. Use it to identify questions that should have clear answers inside your business.

For each item, mark whether you have a clear answer. If you cannot answer a question, that is itself a useful finding.

A healthy IT environment should be known, documented, protected, backed up and planned - not managed by memory or guesswork.

01 Network & Internet

Ask yourself: Do you have an up-to-date network diagram showing internet, firewall, switches, Wi-Fi, VLANs and major devices?

Why it matters: Network visibility reduces troubleshooting time and exposes single points of failure.

02 Firewall & Security

Ask yourself: Do you know which firewall protects the business, how it is configured, and when its firmware/support expires?

Why it matters: A firewall that exists but is poorly managed is not a complete security strategy.

03 Servers & Roles

Ask yourself: Do you have a documented list of servers, their roles, operating systems, IPs, owners and support status?

Why it matters: Unknown or unsupported servers create operational and security risk.

04 User Accounts

Ask yourself: Do you know which user accounts exist, who owns them, and whether old or inactive accounts have been removed?

Why it matters: Access should follow current business roles, not historical employment.

05 Shared Folders & Permissions

Ask yourself: Do you know who can access each shared folder and whether permissions follow least-privilege principles?

Why it matters: Excessive access can turn a small incident into a major data exposure.

06 Wi-Fi

Ask yourself: Are business, guest and sensitive devices separated where appropriate, with strong authentication and documented access points?

Why it matters: A flat wireless environment can create avoidable security and performance issues.

07 Backup

Ask yourself: Are critical data and systems backed up automatically, monitored, and tested through actual restore exercises?

Why it matters: A backup that has never been restored should not be treated as proven recovery.

08 Disaster Recovery

Ask yourself: If a critical server or system fails tomorrow, do you have a documented recovery sequence and realistic recovery targets?

Why it matters: Recovery planning turns downtime from a surprise into a managed event.

09 Cloud Services

Ask yourself: Do you have an inventory of Microsoft 365, Google Workspace, SaaS and other cloud services, including administrators and billing owners?

Why it matters: Cloud services can become business-critical without appearing in a traditional IT inventory.

10 Endpoint Security

Ask yourself: Are laptops, desktops and other endpoints protected, patched and centrally visible?

Why it matters: Unmanaged endpoints are common entry points for malware and credential theft.

11 Software & Licensing

Ask yourself: Do you know which business-critical applications are installed, licensed, supported and dependent on specific servers or users?

Why it matters: Licensing and unsupported software can create both financial and operational risk.

12 IT Documentation

Ask yourself: Could a new IT professional understand your environment without relying on one employee's memory?

Why it matters: Good documentation protects continuity when people, vendors or systems change.

13 Single Points of Failure

Ask yourself: Have you identified systems where one device, server, internet link, person or credential can stop a critical business service?

Why it matters: Resilience starts by knowing where failure would hurt most.

14 IT Risks

Ask yourself: Do you have a prioritized list of current IT weaknesses, their business impact and recommended actions?

Why it matters: Not every weakness deserves immediate spending. Prioritization matters.

15 IT Budget & Roadmap

Ask yourself: Is your IT budget based on documented needs, risks and business priorities rather than urgent purchases?

Why it matters: A roadmap helps prevent repeated, reactive spending on the same problems.

Your IT Infrastructure Self-Assessment

Give yourself 1 point for every item you can answer confidently with current, documented information. Give yourself 0 points if the answer is unknown, outdated or only exists in someone's memory.

Score	What it may indicate
13-15	Strong visibility - focus on optimization, resilience and long-term planning.
10-12	Good foundation - some areas need documentation, testing or improvement.
7-9	Moderate risk - important gaps may affect security, continuity or spending decisions.
0-6	High visibility gap - a structured IT assessment should be a priority.

Important: A high score does not automatically mean your IT is secure. It means you have better visibility. The next step is validating whether the environment is correctly designed, protected and maintained.

The 5 Questions Every Business Should Be Able to Answer

- What systems would stop the business if they failed today?
- Where is our critical data stored, and how would we recover it?
- Who has access to our most sensitive systems and data?
- What are our biggest IT risks right now?
- Where should we invest in IT over the next 12 months - and why?

From Checklist to Clear IT Decisions

If several answers were unclear, outdated or dependent on one person, your business may have a visibility problem - not necessarily a hardware problem.

GA Tech's IT Infrastructure Documentation & Audit service creates a structured picture of your current environment and turns it into practical business information.

Documentation	Network and infrastructure diagrams, server roles, IPs, systems and key dependencies.
Access Review	Users, groups, shared folders, permissions and administrative access.
Infrastructure Review	Servers, network, Wi-Fi, backup, cloud services and endpoint environment.
Risk Findings	Weaknesses, single points of failure, gaps and business impact.
IT Roadmap	Prioritized recommendations for the next 3, 6 and 12 months.
Budget Guidance	A practical view of where IT spending should go first - and what can wait.

Before you buy more IT, understand what you already have.

GA Tech

IT Infrastructure Documentation & Audit

Document. Assess. Optimize. Plan.

Contact GA Tech to discuss an IT Infrastructure Assessment for your business.

gatech-lb.com