BRIGHTADVISOR®

IT Infrastructure Checklist

A Complete Guide to Evaluating Your Technology Environment

4450 S. Rural Rd, Suite B-132, Tempe, AZ 85282 | (602) 497-0277 | brightadvisor.com

Why Infrastructure Assessment Matters

Your IT infrastructure is the foundation every business process runs on. When it works, nobody notices. When it fails, everything stops. A proactive infrastructure assessment identifies aging equipment, security gaps, and single points of failure before they cause costly downtime or data loss.

Most small and mid-sized businesses operate with infrastructure that evolved organically over years of ad hoc decisions, different vendors, and short-term fixes. This assessment gives you a clear picture of where you stand today and what needs attention tomorrow.

> The average cost of IT downtime for a small business is $427 per minute. For a mid-sized company, it exceeds $9,000 per minute. Proactive infrastructure management is significantly cheaper than reactive crisis response.

Signs You May Need Managed IT

If you recognize three or more of these warning signs, it is time for a professional infrastructure assessment.

- Frequent hardware failures, slow computers, or recurring help desk tickets
- Your IT person is a single point of failure (one person holds all the knowledge)
- You are unsure if your backups are working or have never tested a restore
- Employees use personal devices with no management or security controls
- You have no documented disaster recovery or business continuity plan
- Software licenses are managed on spreadsheets (or not managed at all)
- Your server or network equipment is more than 5 years old
- You have experienced a security incident or close call in the past 12 months
- IT costs are unpredictable, spiking with emergencies and break-fix bills
- Onboarding new employees takes days instead of hours

Infrastructure Assessment Checklist

Server & Cloud

Item	Current State	Risk Level	Action Needed

Server age and warranty status (replace > 5 years)			
Cloud migration readiness assessment completed			
Hybrid cloud strategy defined (on-prem vs. cloud workloads)			
Disaster recovery plan documented and tested annually			
Virtualization deployed to maximize hardware efficiency			
Server OS current with active vendor support			
Storage capacity sufficient with 20%+ headroom			
Server room environment controlled (cooling, power, access)			

Network

Item	Current State	Risk Level	Action Needed
Internet redundancy (failover ISP or cellular backup)			
Bandwidth adequate for current and projected needs			
Switches and routers current (replace > 5 years)			
WiFi coverage verified in all work areas with no dead zones			
Network monitoring and alerting tools deployed			

Network documentation current (topology, IP scheme, credentials)			
Guest WiFi isolated from corporate network			
QoS configured for VoIP and video conferencing			

Security

Item	Current State	Risk Level	Action Needed
Firewall current with active subscription and updated rules			
Endpoint protection (EDR) on all devices with auto-updates			
Backup verified with monthly test restores			
Access controls follow least-privilege principle			
Security awareness training conducted for all employees			
MFA enabled on all critical systems and remote access			

End-User Computing

Item	Current State	Risk Level	Action Needed
Workstation age (replace > 4 years for optimal performance)			
Operating systems current with active support (no Win 10 EOL)			

Software licensing tracked and compliant			
Remote work infrastructure tested and secure			
Help desk satisfaction measured (target > 90%)			
Standard hardware/software image defined for consistency			
Employee onboarding/offboarding IT checklist in place			

Business Continuity

Item	Current State	Risk Level	Action Needed
Recovery Time Objective (RTO) defined for critical systems			
Recovery Point Objective (RPO) defined for critical data			
Backup tested with documented restore procedure			
Disaster recovery plan documented and distributed			
Emergency communication plan established			
Cyber insurance coverage adequate and current			
Key vendor and support contact list maintained			

In-House IT vs. Managed IT

One of the most significant infrastructure decisions is whether to keep IT in-house or partner with a managed services provider (MSP). Here is an objective comparison.

Factor	In-House IT	Managed IT (MSP)
Cost	Salary + benefits + tools ($85K-$150K+ for one FTE)	Predictable monthly fee ($100-$250/user/mo)
Coverage	Business hours; on-call overtime is costly	24/7/365 monitoring and support included
Expertise	1-2 generalists; limited specialization	Team of 15-50+ specialists across domains
Scalability	Hiring takes 2-4 months; hard to scale down	Instant scaling up or down with business needs
Tools & Technology	Limited budget for enterprise tools	Enterprise-grade tools included in fee
Single Point of Failure	If your IT person leaves, knowledge leaves	Documented processes; team-based approach
Strategic Planning	Often consumed by daily firefighting	Dedicated vCIO/vCISO for roadmap and budgeting

Getting Started with Managed IT

Transitioning to managed IT does not have to be disruptive. A well-structured onboarding process ensures continuity for your team while systematically improving your infrastructure. Here is the typical five-step process.

1. Discovery & Assessment (Week 1-2): A comprehensive audit of your current infrastructure, including hardware inventory, software licensing, network topology, security posture, and documentation review. This produces a clear baseline and identifies immediate risks.
2. Remediation & Stabilization (Week 2-4): Address critical issues first. This typically includes patching, backup verification, security hardening, and resolving any immediate reliability concerns. The goal is a stable foundation before optimizing.
3. Migration & Standardization (Month 2): Onboard your environment into the MSP's monitoring, management, and help desk platforms. Standardize configurations, deploy management agents, and establish remote support capabilities.

4. Optimization & Documentation (Month 2-3): Implement proactive monitoring and alerting, optimize system performance, complete IT documentation, and establish processes for onboarding, offboarding, and change management.
5. Strategic Planning (Ongoing): Quarterly business reviews with a virtual CIO to align technology investments with business goals, plan hardware refresh cycles, evaluate new technologies, and manage your IT budget proactively.

What to Look for in a Managed IT Provider

- Transparent, predictable pricing with no hidden fees or long-term lock-in
- Proven onboarding process with defined timeline and milestones
- Dedicated account manager and virtual CIO for strategic guidance
- 24/7 monitoring and support with guaranteed response time SLAs
- Cybersecurity expertise integrated into the managed services offering
- Client references in your industry and business size range
- Clear documentation and knowledge transfer so you are never locked in
- Regular reporting on system health, ticket metrics, and project status

> BrightWealth® managed IT services include a complimentary infrastructure assessment for prospective clients. Our team will evaluate your environment, identify risks, and present a prioritized roadmap, all at no cost and no obligation. Contact us to schedule your assessment.