Hypershift

HYPERSHIFT.COM

CHECKLIST

IT ESSENTIALS FOR SMALL & MEDIUM BUSINESSES: A COMPREHENSIVE CHECKLIST

Take Charge Of Your IT Systems & Processes, To Ensure Smooth & Reliable Operations

IT HEALTH CHECK

Technology doesn't just power your business—it is your business. But between helpdesk tickets, security patches, and user management, it's easy to lose track of critical tasks that keep your IT functions running smoothly.

What was secure and efficient three months ago may now be outdated or exposed.

This checklist is designed for IT leaders, business owners or office managers who want clarity on IT functions that should be reviewed regularly - which will keep small issues from turning into major disruptions.

Whether you manage IT internally or partner with a Managed Services Provider (MSP), this checklist will help you stay ahead of performance, risk, and compliance gaps.

Why Quarterly IT Health Checks Matter

IT environments evolve quickly. Whether through software updates, user changes, new vendors, or shifting compliance requirements. What was secure and efficient three months ago may now be outdated or exposed. Without a structured, recurring review process, gaps in visibility can lead to silent failures and misaligned priorities.

Quarterly health checks provide a rhythm for accountability. They help your team catch misconfigurations before they become security risks, review user access before it becomes a compliance concern, and assess hardware and software performance before it impacts productivity.

It’s not just about avoiding emergencies, it’s about making proactive improvements to reliability, security, and efficiency.

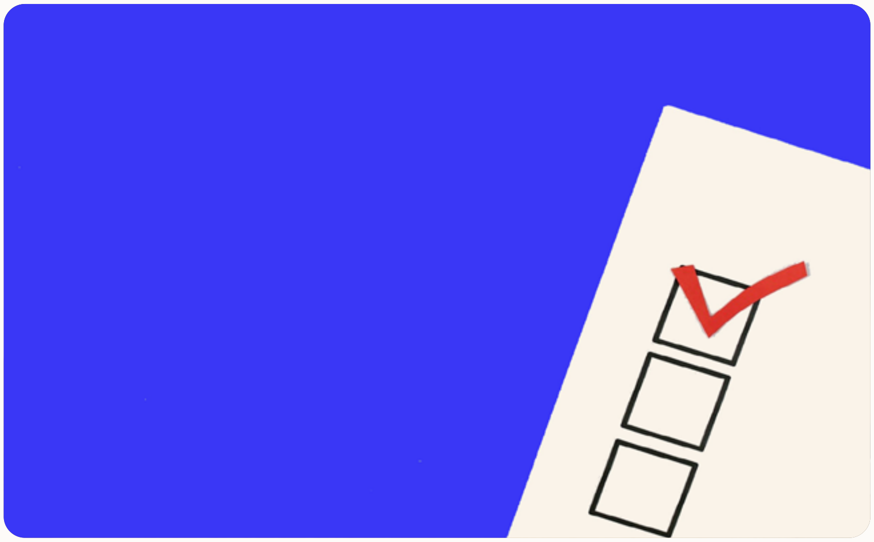
Key benefits of quarterly IT reviews include:

- **Improved Security Posture** – Identify unpatched systems, unnecessary admin rights, or unauthorized devices before they become entry points.
- **Performance Optimization** – Uncover bottlenecks in endpoint, server, or network performance that slow down operations.
- **Regulatory Readiness** – Stay aligned with evolving compliance standards (like HIPAA, GDPR, or NIST) through regular documentation and audits.
- **Cost Control** – Spot underutilized software licenses, overlapping tools, or expiring warranties that can be consolidated or retired.
- **Better Strategic Alignment** – Ensure your IT environment continues to support changing business goals and hybrid work requirements.

Quarterly health checks provide a rhythm for accountability.

Whether you’re scaling up or just trying to maintain a clean IT foundation, quarterly reviews create a baseline for smarter, faster, and more confident decisions.

IT HEALTH CHECK CHECKLIST



Here's a practical checklist for keeping your IT operations secure, stable, and compliant — with or without a Managed Services Provider.

Security ✓

☐ **Essential Identity & Access Management practices are in place,** including MFA being enforced for all users and critical systems.

> Enable MFA for all logins to email, file systems, remote access tools, and administrator consoles. Enforce conditional access policies where available. Prioritize least privilege principles by auditing user roles and group memberships.

☐ **All devices** (servers, workstations, mobile) **are running up-to-date antivirus/EDR.**

> Confirm that antivirus or endpoint detection and response tools are installed, licensed, and actively reporting across your environment. Automate definition updates and enable alerting for quarantined threats, failed scans, or tampering attempts.

□ **Basic Firewall configurations** such as content filters and VPN settings **have been reviewed, adjusted as needed, & tested.**

> Audit inbound and outbound rules for open ports and allowed IP ranges. Review VPN access logs, confirm split-tunnel vs. full-tunnel configurations, and test geo-blocking and application filtering policies.

□ **Security patches have been applied across all systems** - both critical applications and Operating System patches.

> Use patch management tools to deploy OS and third-party application updates. Scan regularly for missing patches and apply critical security updates on a defined cadence. Maintain a rollback plan for problematic updates.

□ **Users have completed cybersecurity awareness training** in the past 6 months.

> Assign training modules on phishing, credential hygiene, and safe browsing. Reinforce key topics with simulated phishing tests and quarterly refreshers. Track completion and reassign as needed for new hires or non-compliant users.

□ **Run monthly email phishing simulations** with low-cost tools like KnowBe4 or Microsoft Defender Attack Simulation to test and improve employee awareness.

> Simulated attacks help reinforce awareness and measure progress over time. Adjust future training based on user behavior to reduce the risk of successful phishing attempts.

□ **Turn on security and system logging for servers, cloud apps, and firewalls. Even basic email alerts for failed logins or disk errors can help spot early issues.**

> Enable logging across critical systems and set up automated alerts for anomalies. This provides early visibility into potential threats or hardware failures before they escalate.

Data Backup & Disaster Recovery ✓

□ **Backups are important** even if all of your data is in the cloud.

Most SaaS providers do not protect you from accidental deletions or ransomware encryption. Implement third-party cloud backup tools for Microsoft 365, Google Workspace, and cloud file storage platforms.

□ **Backups are tested quarterly** for data integrity and recoverability.

Perform test restores of both full systems and granular files. Review logs for failed jobs and validate backup job completion rates. Document the testing process and assign accountability.

□ **Your Disaster Recovery Plan,** RTO (Recovery Time Objective), and RPO (Recovery Point Objective) **align with current business needs**.

Review how much downtime (RTO) and data loss (RPO) your business can tolerate. Adjust infrastructure, backup frequency, and recovery automation to meet those thresholds. Align DR goals with compliance and operational expectations.

□ **Keep a secure, offline file (or password vault entry)** with key system access credentials, support vendor contacts, and recovery instructions in case you're unavailable.

This ensures continuity if your main IT contact is unreachable. Secure offline storage (like an encrypted USB or password manager with emergency access) helps during outages or emergency recovery.

□ **Document your top 10 critical systems** (email, finance, backups, etc.), **note where they live, and who to call if they go down.**

This simple exercise dramatically improves recovery speed. Assign ownership for each critical system and update contact lists regularly.

Systems & Infrastructure ✓

□ **Servers and workstations** are patched, monitored, and performing within normal ranges.

Ensure all endpoints receive regular OS and application updates (e.g., Windows Updates, driver patches). Use centralized tools (like RMM, Microsoft Intune, or WSUS) to monitor device performance, uptime, CPU/memory usage, and failure alerts. Devices that deviate from baselines should be flagged for review or replacement.

□ **Unused systems and user accounts** have been de-provisioned across both cloud and on-premise systems.

Regularly audit Active Directory, Azure, Microsoft 365, and SaaS apps for stale or inactive accounts. Ensure decommissioned servers or VMs are properly removed and no longer consuming resources or exposing open ports. Apply termination checklists and automate offboarding workflows where possible.

□ **Cloud storage usage and file-sharing permissions are reviewed** quarterly to ensure alignment with security best practices.

Review OneDrive, SharePoint, Google Drive, and Dropbox permissions for publicly shared or externally accessible content. Identify over-allocated quotas, unauthorized links, and misconfigured folder-level permissions. Clean up orphaned content from departed users to maintain control and visibility.

□ **Licenses and subscriptions** (e.g. Microsoft 365, antivirus) are current and right-sized.

Review your current license usage and adjust based on actual user count and feature utilization. Cancel or downgrade unused services and ensure upcoming renewals align with business needs. Monitor security and productivity suites (like M365 E3/E5, Defender, or Google Workspace) to eliminate waste.

□ Firewalls, routers, and switches often run outdated firmware. **Set a calendar reminder to check for firmware updates from your hardware vendors every 90 days.**

Firmware vulnerabilities are often overlooked but can be exploited. Updating network gear ensures performance improvements and closes known security holes.

□ **Perform a walkthrough of your office to physically** inspect endpoints, printers, Wi-Fi access points, and backup drives.

Look for warning indicators like blinking red lights, disconnected cables, outdated operating systems, or signs of physical damage. Don’t let hardware failures go unnoticed due to inattention.

IT Strategy & Support ✓

□ Ticket resolution metrics and user satisfaction **are being tracked**.

Use helpdesk tools (like Zendesk, Freshservice, or Autotask) to measure time-to-resolution, first-contact resolution, and backlog. Capture user feedback through CSAT or NPS surveys. Look for trends in recurring issues and use them to inform training or root cause fixes.

□ **Documentation (network maps, logins, key systems) is up to date** and complete across your whole environment.

Maintain centralized documentation for IP schemas, credentials (stored securely), software inventories, vendor contacts, and business-critical apps. Use platforms like IT Glue or Hudu to standardize and secure access. Ensure it’s accessible during outages or emergencies.

□ Quarterly business review (QBR) or IT roadmap meeting **has been completed**.

Schedule regular alignment meetings with IT stakeholders or your MSP to assess goals, pain points, and upcoming initiatives. Use these reviews to evaluate IT investments, prioritize remediation efforts, and ensure strategic alignment between technology and business objectives.

□ **Minimize risk** by reviewing admin rights monthly on local machines, cloud platforms, and business apps.

Apply the principle of least privilege by limiting administrative access to only those who need it. Use role-based access controls and regularly audit changes to admin group memberships.

□ Deactivated employees often linger in email systems, cloud storage, and software tools. **Regularly archive or delete unused accounts to cut costs and limit access points.**

Inactive accounts can create shadow IT risks and increase your license spend. Implement offboarding procedures that include disabling access across all platforms and removing unnecessary data retention.

Bonus Tip: Don’t Go It Alone ✓

Checking the boxes is just the beginning. Knowing how to optimize, automate, and secure your environment is where the real value comes in—and that’s where Hypershift can help.

We partner with organizations like yours to:

✓ Monitor and manage systems 24/7.

✓ Reduce risk through layered security.

✓ Keep IT aligned with growth and budget goals.

✓ Help organizations meet compliance requirements for standards like NIST, SOC 2, and CMMC — with expert guidance tailored to regulated industries.

Ready for a second set of eyes?

Book a discovery call and see how we help.

ABOUT HYPERSHIFT

We're dedicated to championing businesses' digital evolution. Our team offers top-tier consulting on new and emerging technologies, encompassing enterprise infrastructure, cloud solutions, networking, security, and analytics.

Let us pave the way for your organization to keep moving forward. Our experts are well-versed in both traditional data centers and modern cloud environments. We guide businesses in seamlessly integrating these platforms, ensuring a tailored approach that aligns with their unique objectives.

While we specialize in mid-sized companies, we have partnered with companies of all sizes, including Fortune 100 giants. Our Hypershift managed service division is trusted by over 160 financial institutions. We take pride in being a part of CISA's critical security infrastructure initiative, which helps safeguard organizations.

Our team is our secret weapon. With 6 CCIE-certified engineers (some who've even earned it multiple times) and over 50 experienced consultants, we have the expertise to handle any size organization.

We can confidently manage even the most complex networks with efficiency and precision.

We don’t go it alone. With over 70 industry-leading partners, such as Cisco and Nutanix, we offer a comprehensive range of solutions and consulting services.

Let Hypershift be a trusted partner in pushing your organization forward with better technology.

hello@hypershift.com

Hypershift

HYPERSHIFT.COM