

Annual IT review checklist

Summary

- ⑩ An annual IT review helps you check whether your technology is safe, dependable and fits your needs.
- ⑩ The guide covers IT equipment, cybersecurity, user access, backups and recovery.
- ⑩ It also helps you review software licences, cloud services, GDPR and data protection.
- ⑩ Internet, Wi-Fi, network performance and IT costs should be reviewed regularly.
- ⑩ Outdated policies, devices, unused licences and former employee accounts can create risks.
- ⑩ The guide highlights mistakes and gives quick wins to improve IT security and reliability.
- ⑩ A practical 30-day plan helps you review, secure, improve and plan your IT.
- ⑩ Regular IT reviews can reduce risks, control costs. Prepare your business for future growth.



What Achieve

You'll

- Identify IT risks and weaknesses soon, as possible.
- Improve security measures, backups and user access controls.
- Cut down on IT expenses.
- Make sure systems are dependable and always current.
- Make a 12-month IT improvement plan.

1. Review Your IT Equipment

Why it matters

Old or unreliable computers, laptops, printers and networking equipment can reduce productivity and increase the risk of failures.

Checklist

What to review
☐ List all computers and laptops
☐ Check the age and condition of devices
☐ Identify devices that are slow or unreliable
☐ Check warranty and support status
☐ Review monitors, printers and other equipment
☐ Replace equipment approaching the end of its useful life
☐ Securely dispose of old devices

Minimum: Know which equipment the business owns.

Better: Keep an up-to-date list of assets.

Best: Plan replacement cycles so that equipment is replaced before it breaks.

2. Check Cyber Security

Why it matters

Cyber threats change all the time. Security measures that were good year may not protect enough now.

Checklist

- ☐ Make sure antivirus and endpoint protection are running.
- ☐ Check that operating systems and software are getting security updates.
- ☐ Review firewall protection.
- ☐ Make sure multi-factor authentication (MFA) is turned on where possible.
- ☐ Review administrator accounts.
- ☐ Remove accounts and access permissions.
- ☐ Check if important systems still use shared passwords.

Review phishing and security awareness training.

Check if your organisation should get or renew Cyber Essentials.

Minimum: Basic security controls are turned on.

Better: MFA, strong access controls and regular security reviews are, in place.

Best: security testing and a documented cyber-security improvement plan.

3. Review User Access

Why it matters

Employees change roles join or leave the business and take on new duties. Old accounts or many permissions can create security risks.

Checklist

Review	Action
User accounts	Remove accounts no longer required

Leavers	Confirm access has been removed
Permissions	Check users only have access they need
Admin accounts	Limit administrator privileges
Shared accounts	Identify and replace where possible
MFA	Confirm it is enabled
Passwords	Review password policies

Minimum: Remove access when someone leaves the organisation.

Better: Review permissions once every year.

Best: Use role-based access. Conduct regular access reviews.

4. Review Backups and Recovery

Why it matters

Backup is only useful if it can actually be restored. An annual IT review should check that your important business data is protected and that recovery procedures still work.

Checklist

- ☐ Identify business data.
- ☐ Confirm data is being backed up.
- ☐ Check frequency.
- ☐ Check that backups are protected from ransomware.
- ☐ Review where backups are stored.
- ☐ Test restoring files from backup.
- ☐ Check how critical systems could be recovered.
- ☐ Review your disaster recovery plan.

Minimum: Critical data is backed up.

Better: Backups are. Regularly tested.

Best: Maintain tested recovery procedures with defined recovery priorities.



5. Review Software and Licences

Why it matters

Software: Businesses often pay for software they no longer use. At the time important applications may have expired licences or unsupported versions.

Checklist

- ☐ List the software used by the business.
- ☐ Review subscriptions.
- ☐ Cancel licences.
- ☐ Check renewal dates.
- ☐ Check whether software is still supported.
- ☐ Review duplicate applications doing the job.
- ☐ Check whether staff actually use the tools being paid for.
- ☐ Review software costs against business needs.

Minimum: Keep software licensed and supported.

Better: Review subscriptions annually.

Best: Track licences centrally. Review usage before renewals.

6. Review Cloud Services

Why it matters

Cloud services: Many UK businesses depend on cloud services for email, file storage, accounting, collaboration and customer management. Losing access, to a cloud account can seriously disrupt operations.

Checklist

- ☐ Review all cloud services currently being used.
- ☐ Identify who owns each account.
- ☐ Check administrator accounts.
- ☐ Enable MFA.
- ☐ Review external sharing.
- ☐ Remove users who no longer require access.
- ☐ Check storage usage.
- ☐ Review subscription levels.
- ☐ Confirm cloud data is appropriately protected.

7. Review GDPR and Data Protection

Why it matters

Your IT systems hold information. This includes data about customers, employees and suppliers. Your annual review gives you a chance to make sure this information is treated properly.

Checklist

- Check what data the business keeps.
- See who has access to that data.
- Look at how the data is kept.
- Make sure old data is securely deleted when no longer needed.
- Go over your privacy notices and statements.
- Take a look at your data protection rules and processes.
- Check the data processors and any third-party services you use.
- Confirm if your ICO registration or details need updating.

When reviewing, use guidance from the Information Commissioners Office (ICO) wherever



8. Review Internet, Wi-Fi and Network

Why it matters

Internet speed or unstable connections can slow down work across the whole business. Reliable connectivity is essential for day-to-day operations.

Checklist

- Test internet. Check how stable the connection is.
- Check the broadband contract. Note when it's due for renewal.
- Look at your business Wi-Fi coverage—make sure it reaches all areas.
- Make sure guest Wi-Fi is separate from business systems.
- Review the settings, on your router and firewall.
- Replace networking gear that may be slowing things down.
- Consider whether having a backup internet connection makes sense.

Minimum: A business internet and secure Wi-Fi setup.

Better: Use business-grade equipment. Keep guest Wi-Fi separate.

Best: Add network monitoring build in resilience and keep a record of your network configuration.

9. Review IT Costs

Why it matters

Technology costs can slowly increase through subscriptions, licences, support contracts and unused services.

Annual cost review

Cost area	Review
Software	Are all licences being used?
Cloud storage	Is the current plan suitable?
Internet	Is the contract still competitive?
Hardware	Are replacement costs planned?
IT support	Is the level of support appropriate?
Security	Are important protections covered?
Mobile services	Are all business connections required?
Backups	Is the current solution reliable and cost-effective?

Don't focus only on reducing costs. The goal is to make sure **money is being spent on IT that supports the business and reduces risk.**

Common Mistakes to Avoid

1. Only checking IT when something breaks

An annual IT review should be proactive of waiting for failures because catching problems early saves time and money.

2. Renewing everything automatically

Do not automatically renew IT subscriptions without checking if they are still needed.

3. Assuming backups work

An IT backup that has never been tested may not help when it is actually needed.

4. Ignoring old devices

Old IT equipment can become unreliable. May no longer receive important security updates.

5. Forgetting former employees

Old IT accounts can remain a security risk if access is not removed properly.

6. Focusing on technology

Your IT review should also consider people, processes, security, costs and business goals.

A 30-Day IT Review Plan

Week 1. Understand	Week 2. Secure
⑩ List hardware. ⑩ List software and cloud services. ⑩ Identify business systems. ⑩ Review IT costs.	⑩ Review user accounts. ⑩ Check IT MFA. ⑩ Update IT software. ⑩ Review IT security controls. ⑩ Check IT status.
Week 3. Improve	Week 4. Plan
⑩ Test IT backups. ⑩ Replace or repair problem IT devices. ⑩ Remove IT licences. ⑩ Improve network or Wi-Fi issues. ⑩ Update IT policies.	⑩ Prioritise remaining IT risks. ⑩ Set an IT budget. ⑩ Plan IT hardware replacements. ⑩ Schedule IT security reviews. ⑩ Create an IT improvement plan, for the 12 months.

About This Guide

This guide has been written by **Computer Support Centre** to help UK small businesses review their IT each year. It provides a practical checklist covering security, equipment, backups, software, cloud services and IT costs. The guide is designed for business owners and directors who may not have a background. It helps businesses identify IT risks and understand what needs attention. Computer Support Centre created this guide to make annual IT reviews easier, clearer and more manageable.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:

□ <https://computersupportcentre.com>

Conclusion

An annual IT review helps your business keep its technology secure, reliable and suitable for its needs. By checking equipment, security, backups, software, cloud services and user access you can identify problems early.

Reviewing IT costs also helps avoid paying for services or licences that are no longer needed. Regular reviews can reduce risks improve productivity and help your business prepare for growth. Use this checklist every year to keep your IT organised, secure and ready, for the 12 months.