ramsac
the secure choice

Everything an Office Manager needs to know about IT

Introduction

If you're an Office Manager who's found yourself suddenly responsible for "looking after IT", you're not alone. In many growing organisations, day-to-day technology oversight often lands with the most organised person in the business, and that's frequently you. You might not have a technical background, but you're now the go-to person for anything from printer problems to cyber risk planning, and that can feel daunting.

This guide is designed to support you. It's not a technical manual, and it's not about turning you into an IT expert. Instead, it's a practical, honest look at what you should be thinking about, the key processes to put in place, and how to work effectively with an external IT partner. We'll explain common terms, highlight risks to watch for, and help you feel more confident in conversations about your organisations IT.

Most importantly, we want to help you spot the difference between ticking the box and genuinely good IT support. Not all managed service providers are created equal, and the right partnership should make your job easier, not add more to your plate.

CONTENTS

Cybersecurity

As organisations rely more heavily on digital tools and hybrid working, cyber threats have become a constant risk. From phishing emails to ransomware attacks, it's essential to have the right protections in place to keep your data, systems, and people secure.

- Ensure robust cybersecurity measures are in place, including firewalls, antivirus software, and regular updates.

- Implement regular cybersecurity training for employees to recognise phishing attempts and other threats. Remember the ISO mandated that all staff and volunteers that have access to data, should receive cyber awareness training as part of their induction, within 30 days of starting and before the employee is granted access to any databases containing personal or sensitive data.

- Implement MFA (Multi-Factor Authentication) across the whole organisation for email, remote logins, and any critical systems.

- Introduce a password management solution to stop people using weak, compromised, or reused passwords. These secure, encrypted platforms generate and store complex passwords, removing the need for individuals to memorise passwords and reducing the risk of them saving passwords in web browsers or writing them down.

- Keep all software and systems updated with the latest security patches and software updates as soon as they are available.

- Regularly review staff's access especially if they change roles or departments. When staff members leave ensure their access to your systems is removed immediately.

All of this is delivered by our award winning, friendly team of IT experts who are focused on ensuring that end users get the best possible experience out of your IT investment, for a fixed monthly cost with no hidden surprises.

Incident Response & Disaster Recovery

Develop and maintain an incident response (IR) plan that outlines the steps to take if a cyber incident is suspected. This should form a part of your overall Business Continuity Plan. An Incident Response (IR) plan typically includes several key components to ensure effective management of cybersecurity incidents. It is important that you practice the plan regularly to ensure everyone knows their roles and the details are constantly kept up to date.

This plan should designate roles such as:

- Who calls the IT provider?
- Who communicates with customers if data is compromised?
- Who has authority to shut down systems to contain an attack?

This plan should also provide a checklist of actions for various scenarios such as:

- What happens if particular software cannot be accessed?
- What happens if the phone system goes down?
- What happens if the Wi-Fi is compromised?
- What is the process for a single machine attack?
- What are the steps if a ransom is demanded?

A good MSP will be able to help you draft an Incident Response Plan and help you reach Cyber Essentials or Cyber Essentials Plus accreditations, both of which can help you to gain the right level of Cyber Insurance coverage for your business. Giving you a little more comfort that you are protected if you were the subject of a cyber threat.

CYBER ESSENTIALS CERTIFIED

ramsac

Action plan:
What to do in the event of a cybersecurity breach

Chances are now high that most organisations will fall victim to cybercrime. So, being prepared is essential for your continuity.

Download cyber response & recovery strategy guide

ramsac
the secure choice

Working with an MSP

A MSP (Managed Service Provider) is a company that remotely manages a customer's IT infrastructure and end-user systems on a proactive basis. If you have one in place you should be assigned an account manager, make sure you have their contact information and introduce yourself. Your account manager will be able to give you a run down of what you can expect from the MSP in a hassle free, jargon free way. It will be key to gain some information from them which will make requests and issues easily to deal with and resolve in the future, and the more you can share the better they will be able to assist you.

You will always have common IT issues which pop up in any organisation; forgotten passwords, Wi-Fi connections, printer issues, emails not sending/receiving, accessory issues (keyboards, mice, etc) and more. Your MSP should be your first point of call for these types of problems, and your account manager can help you understand the best way to log tickets, how to escalate urgent matters, and what information to include to get quicker resolutions. Knowing how to engage effectively with your MSP from the start will save time and reduce frustration, helping you get back to work faster when issues arise.

Information to ask your MSP:

- **IT Support and Maintenance:** What ongoing support and maintenance is in place for your IT systems, including troubleshooting and resolving issues?
- **SLA:** Check the specifics of the SLA. SLAs set clear expectations for both the service provider and the customer, ensuring everyone is on the same page regarding service quality and performance
- **Monitoring and Management:** Are they monitoring your IT infrastructure to ensure everything is running smoothly and to detect potential problems before they become critical?
- **Security:** What cybersecurity measures have they implemented and manage to protect your systems and data from threats?
- **Backup and Disaster Recovery:** Are they ensuring that your data is regularly backed up and can be quickly restored in case of a disaster?
- **Consulting and Strategy:** Do they offer strategic advice on IT investments and help plan for future technology needs? How often are you able to meet with them?

Information to share with your MSP:

Who’s Who: Outline key influencers, people who can sign off changes and the escalation paths.

Business Objectives: Outline your goals and how IT supports these objectives. This helps the MSP align their services with your strategic priorities.

Current IT Infrastructure: Provide an overview of your existing hardware, software, network configurations, and any cloud services you use.

Security Policies: Share your current cybersecurity measures, policies, and any compliance requirements your business must adhere to.

User Needs: Detail the specific IT needs of your employees, including any specialised software or hardware requirements.

Incident History: Inform the MSP about past IT incidents or recurring issues to help them understand potential vulnerabilities and areas of pain.

Budget Constraints: Discuss your budget for IT services to ensure the MSP can tailor their offerings to fit within your financial limits.

Growth Plans: Share any anticipated changes or expansions in your business that might impact your IT needs.

If you do not have a strategic roadmap for your IT growth plans your MSP account manager will be able to create this with you using the above information.

Asset Management

Creating an asset management system is a crucial step in effectively managing your organisation's IT resources. An asset management system is a list of all your IT equipment including computers, laptops, servers, printers, keyboards, mice, and anything else related to the IT system.

- **Decide how you will track assets, you can select an asset management tool that fits your needs. Popular options include Microsoft Intune, ServiceNow, and Asset Panda, or you can create your own system.**
- **Once you have your system established, record detailed information for each asset, such as serial numbers, purchase dates, warranties, locations and owners.**
- **Group assets into categories such as hardware, software, accessories to help your search function later down the line.**
- **Use asset tags or barcodes to uniquely identify each asset.**
- **Regularly update the asset database to reflect changes.**
- **Review and update the asset management system periodically to improve efficiency.**
- **Automate processes where possible to reduce manual effort and improve accuracy.**
- **Check who provides which services to your organisation and keep a record of contacts.**
- **Don't forget to include contact information, account numbers and renewal dates.**

Introducing an asset management system supports ISO compliance while also strengthening health and safety standards. This leads to a more organised, efficient, and secure working environment.

Licensing & Renewals

What you need to know and do

IT licensing might feel like just a little extra admin, but staying on top of it is crucial. If a licence expires or a renewal is missed, you can suddenly lose access to email, files, critical apps — or worse, fall out of compliance with legal or security requirements.

As Office Manager, you're ideally placed to keep things organised and prevent last-minute panics. Here's how to take control:

1 Know What You've Got

Start by asking your MSP for a full list of what your business is currently using. At a minimum, this should include:

- Microsoft 365 (email, Teams, Office apps)
- Antivirus and cybersecurity tools
- Cloud backup and recovery services
- Line-of-business apps (anything industry-specific)
- Domain name registration and website hosting
- Hardware warranties or support contracts

Make sure each item includes the number of licences, who they're assigned to, and renewal dates.

2 Track Renewal Dates

Set up a shared calendar or spreadsheet with key dates at least **30–60 days before renewal.** This gives you time to review:

- Are you still using all the licences?
- Are you paying for more than you need?
- Is there a better or more secure option available?

A proactive MSP will help you with this, but it's worth having your own visibility — especially for budgeting purposes.

Licensing & Renewals

What you need to know and do

3 Review Usage and Costs

Over time, it's easy for costs to creep up. Staff leave but licences stay active, or new tools are added without consolidating others.

Do a simple check every quarter:

- Who is using what?
- Are there any duplicates or overlaps?
- Could you reduce costs by switching plans or consolidating services?

Again, your MSP should provide usage reports and honest advice on value for money.

4 Be Aware of Compliance Risks

Using unlicensed or expired software poses serious risks, including legal penalties and reputational harm. In addition, such software is often unsupported and insecure, potentially putting organisations in breach of industry standards like GDPR and Cyber Essentials, which require robust cybersecurity and risk management controls.

Ask your MSP to confirm:

- That everything in use is properly licensed.
- That renewals are automatically tracked and managed.
- That you're not inadvertently using trial or consumer-grade software in a business setting.

5 Have a Simple Audit File

Create a digital folder where you keep:

- Licence agreements or invoices.
- Renewal confirmations.
- Any correspondence about upgrades or changes.
- A clear contact list: who to speak to at the MSP if something needs updating.

This gives you peace of mind if a finance director, auditor, or insurer ever asks for proof.

Policies

A key to keeping your IT estate secure and functioning efficiently is to develop and enforce security policies ensuring that IT systems and practices comply with relevant regulations and standards. Key policies and procedures to have established are:

- A Cybersecurity Policy (or a set of policies) that outline how the organisation manages and protects information. A cybersecurity policy doesn't need to be hundreds of pages; it can be a concise document covering areas like acceptable use of organisation devices, password requirements, data handling procedures, incident reporting, and so on.

- A Data Breach Response and Notification Policy goes hand-in-hand with the incident response plan. A clear policy on how to handle data breaches, especially regarding notifications, should define what constitutes a notifiable breach and assign responsibility for making that decision and drafting notifications.

- A Third-Party/Supply Chain Security Policy Develop policies or guidelines about engaging with third-party vendors from a security standpoint. This could involve requiring contracts to include data protection agreements, setting up Non-Disclosure Agreements (NDAs) when giving contractors access to sensitive info, and having criteria for selecting tech suppliers. In sectors like defence or critical infrastructure, formal supplier vetting is required; even if not mandated for your SME, adopting a scaled-down vetting for your key suppliers is wise. Essentially, treat your suppliers as an extension of your enterprise and insist on certain standards, even if it's just verbal confirmations.

Implementing and enforcing these policies creates a strong foundation for cybersecurity. They ensure that there is organisational clarity and commitment to security. Cyber threats evolve quickly, so policies should not be static, they should instead be periodically assessed and updated accordingly.

If you have an MSP in place they may be able to support you in writing Cyber based policies to ensure all the important points are hit and you have coverage for all possible eventualities.

Strategic IT Planning

Why it matters and what to cover

Even if you're not setting the IT strategy yourself, you play a key role in keeping the business aligned, organised, and future-ready. Strategic planning ensures your tech keeps pace with how the organisation works — and that you're not constantly reacting to problems.

Here's what to keep on your radar:

1 Upcoming Needs

Work with your MSP to review:

- When devices are due for replacement
- Any software reaching end-of-life.
- Whether storage, security, or remote access needs are evolving.

Proactive planning avoids sudden costs or operational disruption.

2 Budgets and Roadmaps

Ensure IT spend is forecast properly — especially for larger projects like system upgrades, server replacements, or office moves. Ask your MSP to provide a simple 12–24 month roadmap with expected costs and priorities.

3 Review Usage and Costs

Has the team gone more hybrid? Is collaboration suffering? Strategic planning is about aligning technology with how people want (and need) to work. IT should enable that, not hold it back.

4 Regular Reviews

Set time every 6–12 months for a non-technical review meeting with your MSP. This should cover:

- What's working well
- What's on the horizon
- Any risks or recommendations

If your current provider isn't offering this kind of input, it might be time to ask why.

Conclusion

Taking responsibility for IT as an Office Manager can feel like a steep learning curve — especially if it's not your background. But with the right processes in place and the right support around you, it's a role you can manage confidently and effectively.

This guide has outlined the key areas to focus on — from cybersecurity and licensing to backups, planning, and support. You don't need to become an IT expert, but you do need to know what good looks like. A reliable, proactive MSP should be making your job easier, not more complicated. If you're constantly chasing answers, unsure what's being looked after, or not getting clear advice, it's reasonable to question whether your current provider is meeting the mark.

Ultimately, strong IT management is a team effort. Your role is about coordination, clarity, and keeping things moving — and when you're backed by a trustworthy IT partner, you'll be empowered to do just that.

IT Action Plan Checklist

Download the essential IT health check

Weekly

□ **Check the IT support log or ticket system**

Review outstanding issues. Chase unresolved tickets if needed and spot any recurring problems.

□ **Follow up on new starter/leaver/change requests**

Ensure users have the right access, licences, and equipment — or that access has been removed promptly.

□ **Remind staff to report issues**

Reinforce the process for logging IT problems to avoid shadow IT or underreporting.

Monthly

□ **Meet (briefly) with your MSP or IT lead**

Get a quick update: what's happened, what's coming up, any concerns?

□ **Review cybersecurity status**

Confirm that antivirus, patching, and backups are running as expected (your MSP should provide this).

□ **Check for pending renewals**

Look ahead 1–2 months for any software or licence renewals, especially domain names, Microsoft 365, antivirus, etc.

□ **Update your user/device list**

Keep your records accurate — who has what equipment, and what licences are assigned.

Quarterly

□ **Review IT spend and usage**

Are you paying for unused licences? Are there cost-saving opportunities or duplicate tools?

□ **Run a basic IT hygiene check**

Work with your MSP to confirm:

- □ Backups are working and tested
- □ Devices are updated and supported
- □ No risky or unsupported software is in use

□ **Update your IT documentation**

Ensure records of logins, licences, support contacts, and procedures are current and accessible (ideally in a secure shared folder).

□ **Get staff feedback on IT performance**

Are tools working well? Are there recurring frustrations? Share with your MSP.

Annually

□ **Plan for the year ahead**

Review your MSP's roadmap: expected projects, device replacements, security updates, budget forecasts.

□ **Hold a strategic review with your MSP**

Discuss business goals, changes in working patterns, and how technology can support the organisation.

□ **Test your disaster recovery plan**

Make sure your MSP can walk you through how long recovery would take if systems went down.

□ **Review your MSP's performance**

Are they responsive? Proactive? Do they explain things clearly and take the pressure off you? If not, it might be time to explore alternatives.

About ramsac

ramsac is an IT support and managed services provider based in Surrey. We offer a proactive 24-hour service which cuts the stress out of managing technology. Whether it's designing a new infrastructure, migrating services to the cloud, implementing a new phone system or providing end users with really efficient and friendly IT support, ramsac manages IT on your behalf, so that you can focus on achieving your organisation's goals, safe in the knowledge that IT is secure, staff are working efficiently, and the IT investment is delivering tangible benefits to the organisation.

Most importantly, we want to help you spot the difference between ticking the box and genuinely good IT support. Not all managed service providers are created equal, and the right partnership should make your job easier, not add more to your plate.

We help our clients to get the best out of technology – implementing, managing and supporting secure, resilient, flexible IT solutions. We work with small and mid-sized organisations, providing them with strategic IT input, proactive management, jargon-free IT support and solutions that help them to grow their own organisations efficiently and securely.

Find out more

We would love to talk to you about your specific needs and to discuss whether you might benefit from a free IT health check.

To book an initial consultation:

Call: 01483 412 040

Email: info@ramsac.com

Visit: www.ramsac.com

ramsac
the secure choice