Choosing a managed service provider (MSP)

An SME's guide to selecting and working with managed service providers.

Many small to medium-sized enterprises (SMEs) use managed service providers (MSPs) to deliver IT products and services, manage important data, and to provide cyber security. This guidance describes how to select and work effectively with MSPs, and includes a checklist you can use when sourcing MSPs.

> **Note:**
> If you're part of an IT team responsible for working with MSPs within larger organisations (over 250 people), you should refer to the NCSC's more detailed Cloud Security Guidance.

Introduction: SMEs are at risk

UK organisations are increasingly targeted by cyber criminals. This can can result in financial loss, service disruption, and damage to organisations' reputations.

Since MSPs will have access to your systems and data (which could include your customers' details), it's important to ensure that MSPs take cyber security seriously, and that you understand the measures they have in place. This means asking the right questions when contracting an MSP to ensure your data, systems, and reputation are protected. A proactive approach – where cyber security is considered when you're selecting your MSP – reduces the risk of costly data breaches, service downtime, and regulatory penalties.

Choosing an appropriate MSP

By proactively engaging and scrutinising MSPs, SMEs can better protect themselves, their customers, and their data. This section describes what to look for when selecting an MSP.

Certifications matter

You should use MSPs with recognised certifications such as **Cyber Essentials Plus**, the UK government's minimum baseline standard for cyber security. You can use the Cyber Essentials website to check if your MSP is certified. Choosing an MSP that is certified is important because it acts as a quality and trust indicator. Other certifications like ISO 27001 or SOC 2 demonstrate an organisation takes information security seriously - which includes cyber security.

Even if you're using a certified provider, each service your organisation uses will still need to be *configured* in such a way that it's safe from common cyber attacks. You can use the NCSC's separate guidance to quickly check any online service. Reputable service providers make it easy for you to do this, and will often provide useful 'getting started' tutorials and guides, such as:

- Google Workspace: Security checklist for small businesses (1-100 users)
- Microsoft 365: Top 10 ways to secure your data with Microsoft 365

Check client references

Ask your MSP to provide you with testimonials and/or references from their other clients (particularly SMEs) so you can review current customer feedback. An MSP's track record can be a strong indicator of their reliability and ability to handle security incidents, as well as how they will work with you in the future.

Transparency and good communication

A reputable MSP should clearly articulate the services, policies, and responsibilities they offer. Open communication about security incidents (ie how they are handled and reported) and a swift response is critical to maintain trust. Transparency ensures you're aware of your MSP's practices and their commitment to keeping your environment secure.

Clear contracting

The contract should clearly specify what is and what is not included. A matrix of responsibilities detailing what the MSP will do and what is expected from you as the customer is good practice. When working with a MSP your contract should:

- **Define roles and responsibilities** Clearly set out what the MSP will take responsibility for, and what remains with you as the customer.
- **Agree on incident reporting procedures** Specify how incidents will be reported, including whether the MSP will notify you if they experience one.
- **Establish liability terms** Ensure there is clear agreement on who is accountable for vulnerabilities, damages, and incident impacts.
- **Establish technical reporting** Many insurers may ask to see (for example) recent health or configuration reports in order to validate a cyber insurance claim.

Without clear contracts, responsibilities become ambiguous. It's important to keep the dialogue open with your IT service providers, building a positive relationship and developing a better understanding of each others' responsibilities.

Security issues to discuss with your MSP

Your organisation may rely on a number of IT service providers. You should check that the following measures are in place. You should also assess potential cost implications by carefully reading the MSP contract, as some of these features may incur additional charges. Once agreed all these aspects need including in your contract.

Patching and updates

It is vitally important that your MSP keeps software updated and applies security patches swiftly, as these updates include protection from viruses and other kinds of malware. Ask your suppliers about their policy for applying any updates. Our recommendation is that software is patched within 14 days of an update being released (where the patch fixes a critical or high-risk vulnerability).

Backups

Backups are an essential part of an organisation's response and recovery process, and making regular backups (and ensuring you can recover data from them) is the most effective way to recover from a ransomware attack. Therefore it's important to check with your MSP what backup arrangements are in place, how often these are tested and if these suit your requirements. If they (or you) were to suffer a ransomware attack, how would they recover their service and your data? You should also determine how often your data is backed up, where it is stored, and who has access to it.

Access

Is your data (and the data of others which you have responsibility for) being properly protected? Are you able to put 2-step verification (2SV) in place to limit access to your data and services?

Users should only have access to what they need to do their job, and that access should be removed when that job is completed.

You should only give administrative accounts to people that really need them, and ensure they are protected.

Check that MSPs also protect *their* access to *your* systems. They should also have 2SV in place so these important credentials are protected.

Logs

Logging can play a vital role in diagnosing any problems your systems are facing, and in identifying and investigating security incidents. As well as helping to determine if services are running as expected, logging can provide assurance that security controls are working effectively. Logs will also prove invaluable when responding to and recovering from security incidents. So it's important to check with your MSP:

- if logs are being kept for security purposes

- how long these are kept for
- if you (or your incident management provider) can access this logging data if required

Any specific log retention periods required for your business should be detailed in your contract.

Incident response

What will happen if things go wrong? Your MSP should have clear steps on how they will respond to any incidents and how they will engage with you (including what happens if MSPs are themselves impacted by an incident). For larger organisations, our guidance on security operations, monitoring and incident response goes into greater depth.

Details to check in your MSP contract

Clear contracts define who is responsible for each aspect of an incident, helping protect your organisation and making things easier if you experience an attack. Always insist on clear, detailed contracts that specify responsibilities, response times, and liability, including responsibility for any third parties your MSP uses to deliver the service.

Service level agreements (SLAs)

These agreements help establish clear expectations for response times, resolution times, and overall service delivery and help you evaluate your MSP's performance.

Response time refers to the time between logging an issue and your MSP starting to investigate it. For general service requests or minor issues, a response time of 1 business day is standard. For urgent issues, a response time of under 1 hour is standard.

Resolution times, or the time taken to resolve an issue or implement a workaround, can vary depending on the problem's complexity. However, a resolution time of 2–3 business days for routine issues of medium priority is a good starting point.

Note that requesting quicker response times will likely have an impact on your contract costs.

Regular review and reporting

Regular review and reporting is an important element of your contract and helps to give reassurance your systems are safe, healthy, and operating within the rules (rather than just assuming things are fine until something breaks or you face a breach).

Scheduled audits can help verify systems are configured correctly, and can help identify:

- unapplied security patches
- users with unnecessary administrative rights
- weak password policy implementation

Infrastructure health reports can provide you with details that include:

- monitoring and uptime statistics (servers, network, cloud services)
- patch and update compliance
- backup success/failure rates
- security alerts summary (firewalls, EDR, phishing detections)
- highlights with hardware or software issues

Crucially, a health report also creates an auditable trail showing you’ve been checking, recording, and addressing risks. For cyber insurance, insurers may ask to see recent health or configuration reports after a claim.

Incident notification and management

SMEs are often less resilient to downtime because every hour lost can impact revenue, customer service, and reputation. So it's important your contract details the timeframes in which you will be notified of any security breaches or incidents, and that the incident management process is clearly documented. Notification times will depend on the severity of the incident but it should be something that is suitable for your company.

Access and privilege control

Check with your MSP how they manage access into your systems and how those connections are secured (such as VPNs, encrypted tunnels, restricted IP ranges). This helps to limit potential attack routes into your organisation and makes sure all remote access is properly controlled and monitored. We recommend using least privilege (giving your MSP only the permissions needed to do the job), and enforcing 2SV so accounts are harder to hack. Also check how they protect login credentials, particularly administrative ones.

Contract duration and exit clauses

Sets the length of your agreement and what happens if you want to end or change it, including how renewals, renegotiations, or terminations work. Be clear that the contract duration works with your business objectives and gives you flexibility if your organisation changes direction (or you're unhappy with service quality).

End-of-life systems

Planning for systems approaching end of life (EOL) is critical to maintaining security, compliance, and business continuity. Your MSP contract should clearly state who is responsible for tracking EOL dates, advising on suitable replacements or upgrades, and taking necessary action before support ends. Without this agreement in place, there is a real risk that outdated systems will remain in use after the manufacturer stops providing updates.

Once security patches are no longer available, vulnerabilities can quickly be exploited, potentially leading to data breaches, regulatory penalties, and costly downtime. By discussing and documenting EOL responsibilities upfront, SMEs can avoid last‑minute expenses, unplanned outages, and increased cyber risk, while ensuring IT investments remain secure and effective over time.

MSP due diligence checklist

Choosing an MSP

- ✓ **Does the MSP hold recognised security certifications (e.g., Cyber Essentials Plus, ISO 27001)? If not, what security standards do they use?**
- ✓ **Can they provide references, testimonials or case studies from other SMEs?**
- ✓ **Do they have a proven track record of security and service quality?**
- ✓ **Do they demonstrate transparency about their services and processes?**
- ✓ **Are their service levels (response times, uptime) clearly defined in SLAs?**
- ✓ **Do they fit your needs and budget?**

Services to request

- ✓ **Timely patch management for all systems and software**
- ✓ **Automated, off-site data backups and regular testing of restore processes**
- ✓ **Security monitoring and logging, with alerts for suspicious activity**
- ✓ **Use of 2SV across all access points**
- ✓ **Clear incident response and management procedures**
- ✓ **Application of timely security updates and firmware patches**

Contract and agreement considerations

- ✓ **Is there a detailed Service Level Agreement (SLA)?**
- ✓ **Are roles, responsibilities, and liabilities clearly defined?**
- ✓ **Does the contract specify how and when security incidents are notified?**
- ✓ **Are there provisions for regular reviews and reporting?**
- ✓ **Is the principle of least privilege applied to MSP access?**
- ✓ **Are there clauses for managing obsolete accounts and infrastructure?**
- ✓ **Is there a clear process for contract review, renewal, or termination?**

Risk and responsibility

- ✓ **Have you assessed your MSP's supply chain risks?**

MSP's supply chain risks

- ✓ **Are accountability and liability for cyber security incidents explicitly documented?**
- ✓ **Do MSPs have a tested incident response and recovery plan?**
- ✓ **Are backup and disaster recovery procedures outlined and agreed upon?**

✓ Is there a process for regular security training and awareness?

PUBLISHED

24 November 2025

REVIEWED

24 November 2025

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations

Self employed & sole traders