

IT MANAGED SERVICE PROVIDER



Service Overview

Our IT Managed Service Provider (MSP) service delivers comprehensive, proactive and secure management of IT environments for public sector and regulated organisations.

The service goes beyond traditional break-fix support, providing continuous monitoring, preventative maintenance, cyber security controls, user support and strategic guidance. It is designed to improve reliability, reduce risk and ensure IT services actively support organisational objectives, compliance requirements and service delivery.

The MSP service can be delivered as a fully outsourced solution or as a co-managed service, working alongside internal IT teams.

Service Objectives

The objectives of the IT MSP service are to:

- Provide stable, reliable and secure IT operations
- Reduce unplanned downtime and operational disruption
- Strengthen cyber security and resilience
- Improve user experience and productivity
- Support compliance, assurance and audit requirements
- Provide clear visibility of IT performance, risk and cost
- Enable continuous improvement and forward planning

Intended Customers

This service is intended for public sector organisations and suppliers operating in regulated environments, including central government bodies, local authorities, education providers, healthcare organisations, emergency services and organisations delivering services on behalf of the public sector.

The service is suitable for organisations of varying size and complexity, from smaller teams requiring full IT outsourcing through to larger organisations seeking co-managed or specialist support.

Scope of Service

The IT MSP service provides end-to-end management of core IT services and can be tailored to organisational needs.

The scope may include:

- Service desk and user support
- Endpoint and device management
- Server and infrastructure management
- Network monitoring and support
- Cloud platform management
- Cyber security management and monitoring
- Patch management and vulnerability remediation
- Backup, recovery and resilience oversight
- Identity and access management
- IT documentation and asset management
- Service reporting and review

Services can be delivered across on-premise, cloud or hybrid environments.

Service Delivery Approach

The MSP service is delivered using a proactive, structured and standards-based approach. Engagement begins with onboarding and discovery to understand the existing IT environment, business priorities, risk profile and service expectations. Systems, users, devices and dependencies are documented to establish a clear baseline.

Once onboarded, the environment is managed through continuous monitoring using remote management and monitoring tools. Preventative maintenance activities such as patching, updates, health checks and capacity monitoring are carried out on a scheduled basis to reduce incidents before they impact users.

User support is provided through a structured service desk, covering incidents, service requests and changes. Requests are prioritised based on impact and urgency, with clear escalation paths.

Cyber security controls are embedded throughout service delivery, including endpoint protection, patching, access controls and monitoring for common threats. Security posture is reviewed regularly and improved over time.

The service includes regular reporting and service reviews, providing visibility of performance, incidents, risks and improvement opportunities. Strategic guidance and roadmap planning are provided to ensure IT continues to meet organisational needs.

Core Service Components

The MSP service is built from modular components that can be combined to suit organisational requirements:

- Service Desk and User Support Provides responsive support for incidents, requests and changes, improving user experience and productivity.
- Endpoint and Device Management Covers laptops, desktops and mobile devices, including monitoring, patching, configuration and lifecycle support.
- Server, Cloud and Infrastructure Management Includes management of on-premise servers, cloud services and hybrid environments to ensure availability and performance.
- Network Management Supports reliable and secure connectivity through monitoring, fault resolution and configuration management.
- Cyber Security Management Includes baseline security controls, monitoring, vulnerability management and incident support.
- Backup and Resilience Provides oversight of backup processes, recovery readiness and resilience planning.
- Identity and Access Management Supports secure user access through account management, permissions and lifecycle controls.

Value-Added Services

In addition to core operational support, the MSP service can include value-added services that enhance assurance and maturity.

These may include:

- Compliance support aligned to DSPT, Cyber Essentials and similar frameworks
- Microsoft 365 management and optimisation
- Cloud cost and licence optimisation
- IT strategy and roadmap development
- Technology refresh and lifecycle planning
- Security awareness and best-practice guidance
- Support for audits, inspections and assurance activities

Benefits

The IT MSP service reduces operational risk by improving stability, security and consistency across the IT environment. Organisations benefit from predictable service delivery, faster issue resolution and reduced reliance on internal technical resources.

Improved visibility of IT performance and risk supports better decision-making, while proactive management reduces disruption and long-term costs.

Support Levels

Support is available at different levels to reflect organisational size, complexity and risk appetite.

GP IT Services provides tiered support levels to suit different operational needs. Standard Support, included within the core service price, provides remote support during agreed business hours, incident management and routine service requests. Enhanced Support, available at an additional cost, offers extended hours, faster response targets and priority handling. Fully Managed Support is available as a premium option and includes proactive monitoring, service reviews and change coordination. Support costs vary based on user numbers, infrastructure scope and required coverage and are agreed at contract stage.

Pricing Model

Pricing is based on the size and complexity of the IT environment, number of users and devices, scope of services and support level required. Services are typically priced as a fixed monthly fee to ensure transparency and predictable costs. All pricing is agreed prior to service commencement.

Security and Compliance

Security is embedded throughout service delivery. The MSP service supports compliance with UK GDPR, the Data Protection Act 2018, NCSC guidance and relevant public sector standards.

Controls include access management, patching, malware protection and monitoring.

Onboarding and Offboarding

Onboarding includes service initiation, discovery, documentation and deployment of management tools. Offboarding includes structured handover of documentation and transition support to ensure continuity.

Service Availability

The service is delivered remotely across the UK, with on-site support available by agreement. Business hours support is provided as standard, with enhanced availability options available.

Service Outcomes

Outcomes include stable and secure IT operations, improved user experience, reduced downtime, stronger security posture and clearer visibility of IT performance and risk.

Contact and Escalation

Clear contact details, named resources and escalation routes are provided at service commencement to ensure effective and timely support throughout the engagement.

Service Constraints and Dependencies

Customers remain responsible for strategic business decisions and approval of changes. Timely access to systems, users and documentation is required to deliver the service effectively.

Projects, major changes or specialist services may fall outside the scope of the managed service and be delivered separately.

About Us

IT Auxilium Ltd is a UK technology services provider delivering secure, dependable IT solutions where reliability is critical.

Healthcare is a core specialism. Through our dedicated divisions, GP IT Services and Health IT Services, we support General Practices, Primary Care Networks and independent healthcare providers with IT designed for clinical environments and aligned to NHS frameworks and UK security standards.

Beyond healthcare, IT Auxilium applies the same disciplined, security-led approach to all businesses we support. From managed IT and cybersecurity to cloud services and digital transformation, we provide proactive monitoring, clear accountability and responsive UK-based support, acting as a trusted extension of our customers' teams.

Health IT Services & GP IT Services are trading names of IT Auxilium Ltd.

Additional Support Services

Cyber Essentials (Plus) Consultancy & Audit

Our Cyber Essentials and Cyber Essentials Plus Consultancy and Audit service guides organisations through scoping, gap analysis, remediation and certification. We align with NCSC and NHS expectations, managing audits end to end to achieve certification efficiently and with minimal disruption.

NHS Data Security and Protection Toolkit (DSPT) Support

Our NHS Data Security and Protection Toolkit (DSPT) Support service provides structured guidance to achieve and maintain compliance. We assess readiness, address gaps, prepare evidence and support submissions, ensuring alignment with NHS requirements while reducing risk and administrative burden.

Artificial Intelligence (AI) Readiness Assessment and Advisory Service

Our Artificial Intelligence Readiness Assessment and Advisory Service helps organisations evaluate capability, risk and governance before adopting AI. We assess data maturity, security and compliance, providing clear recommendations to enable responsible, safe and value-driven AI adoption.

Microsoft 365 Migration & Onboarding

Our Microsoft 365 Migration and Onboarding service ensures a smooth, secure transition with minimal disruption. We plan, migrate and configure your environment, apply security best practice and support user adoption, enabling organisations to realise value quickly and confidently.

Backup & Disaster Recovery

Our Backup and Disaster Recovery services provide comprehensive protection across endpoints, Entra ID, Microsoft Azure, Microsoft 365 and Google Workspace. We deliver secure, automated and monitored backups with clearly defined recovery options, helping organisations restore systems and data quickly following cyber incidents, accidental deletion or service disruption. Our approach is designed to support business continuity, regulatory expectations and operational resilience, ensuring critical data remains protected, accessible and recoverable when it matters most.

Medical-Grade Cloud Based Temperature/Environmental Monitoring Data Logger System

Our medical-grade, cloud-based temperature and environmental monitoring service provides continuous automated monitoring, real-time alerts and auditable records for regulated environments. It replaces manual checks, reduces risk and supports compliance, inspections and operational assurance across single or multi-site estates.