Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Fully Managed Service

Service description

info@centralnetworks.co.uk
+44 (0)1706 747474
www.centralnetworks.co.uk

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Contents

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Service Overview

Central Networks' Full Manager Support Service is a comprehensive, high-touch solution designed to provide organisations with seamless, proactive, and strategic IT support across their entire estate. This service is ideal for clients seeking not just technical resolution but a true partnership in managing their IT operations, compliance, and growth.

This Service is a complete support function designed to remove any requirement from the client. Ideal for clients without any technical provision or looking to augment an internal team and looking to have this function outsourced.

List of the core features

End User Services	Included	Optional
1st, 2nd & 3rd Line Remote Support	**Yes**	
1st, 2nd & 3rd Line Onsite Support	No	**Yes**
VIP Support	**Yes**	
Extended Support Hours	No	**Yes**
Monitoring and Alerting Service	**Yes**	
Device management	**Yes**	
M365 Management	**Yes**	
Asset Lifecycle Management	**N**o	**Yes**
Incident Management	**Yes**	
Patch Management	**Yes**	
Problem Management	**Yes**	
Change Control	**Yes**	

CENTRAL.
IT'S WHAT WE DO.

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Infrastructure Services	Included	Optional
1st, 2nd & 3rd Line Remote Support	**Yes**	
1st, 2nd & 3rd Line Onsite Support	No	**Yes**
3rd line Onsite Support for P1 Incidents	**Yes**	
Extended Support Hours	No	**Yes**
Monitoring and Alerting Service	**Yes**	
Azure Management	**Yes**	
Asset Lifecycle Management	No	**Yes**
Incident Management	**Yes**	
Patch Management	**Yes**	
Device Configuration Review (CMDB)	**Yes**	
Problem Management	**Yes**	
Change Control	**Yes**	

Backup and Continuity Services	Included	Optional
Backup alerting and Monitoring	**Yes**	
Backup as a Service (including Microsoft 365)	No	**Yes**
Disaster Recovery as a Service (DRaaS)	No	**Yes**
Business Continuity Planning Support	No	**Yes**
Problem Management	**Yes**	
Change Control	**Yes**	

CENTRAL.
IT'S WHAT WE DO.

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Security Services	Included	Optional
MDR (Managed Detection and Response) for Endpoints	No	**Yes**
ITDR (Identity Threat Detection and Response)	No	**Yes**
SIEM (Security Information and Event Management)	No	**Yes**
User Training and Awareness	No	**Yes**
Cyber Essentials/Cyber Essentials Plus as a Service	No	**Yes**
Patch Assurance and Vulnerability Management	No	**Yes**

Professional Services	Included	Optional
Professional Services Days	No	**Yes**
Onsite Technical Attendance	No	**Yes**
Onboarding and Adoption	**Yes**	
Annual Technology Report	**Yes**	
Innovation and Automation Workshops	No	**Yes**
Quarterly Technology Strategy Reviews	No	**Yes**

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Global Services	Included	Optional
Ticketing and Self-Service Portal	**Yes**	
Integrated Ticketing and Self-Service Portal	No	**Yes**
Custom Workflows	**Yes**	
Reporting	**Yes**	
Service and Account Management	**Yes**	
Procurement Services	**Yes**	

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Service Description

Provision of a support service to encompass the identified platforms, devices, locations or users. This includes the following:

1st, 2nd & 3rd Line Remote Support

This service includes the allowance for unlimited incidents and service requests from the end users. Support will be provided remotely via verbal, email or by remote takeover tools as described within the with the Helpdesk Functionality below.

Incidents, service requests or escalations will also be accepted from a member the internal technical teams or any authorised party included within a co-managed environment.

The support will cover all items identified in the agreement from end user and network devices to infrastructure and cloud platforms.

1st, 2nd & 3rd Line Onsite Support

In addition to the remote support, we can provide onsite support as either prebuilt set of days to consumed for ad hoc work, prearrange regular attendance or permanent onsite staff. This service needs to be agreed in advance and charged accordingly.

We include onsite attendance for all P1 infrastructure issues if the need is identified.

Service levels

Definition of the response and resolve targets are as defined in Central Support Patching and Monitoring Schedule.

VIP Support

Included within the support function is the ability add specifics requirements for a number of your users who might require a specific set of responses or alternative workflows depending on their environment, requirements or availability. This ensures a functional service for all our clients and their users. This feature is setup initially throughout the onboarding sessions or view a service request.

Support Availability

Centrals standard operating hours are as fully detailed in Terms of Engagement.

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

In brief, standard operating hours are Monday to Friday 8am to 6pm Excluding UK National Holidays.

Extended Support Hours

In addition to the hours described as standard operating hours Central can extend the hours of this service. An option for 24/7 support for critical, P1, incidents for Infrastructure clients can be made available. We also provide the option for 24/7 support for 1st line support queries.

Planned changes can also be arranged out of hours by request. These can be requested via during CAB meetings, by contacting your account manager or a submitting a service request.

The phone number of out of hours support is to be used for out of hours outage only rather than generic support enquiries.

Monitoring and Alerting Service

Central offer a Monitoring and Alerting service for in scope devices and platforms. Monitoring the health or devices such as servers, workstations and switches to SaaS platforms, network connected devices and WAN/SDWAN environments. These monitors, when trigged can raise tickets, produce emails and trigger workflows within Centrals PSA platform

The Monitoring and Alerting service leverages Centrals RMM platform and its integration with Centrals PSA platform to inform the Helpdesk of any systems not operating within agreed parameters so actions can be taken.

These are not just for states of failure, but also proactive measures, such as disk space consumption and server service interruptions, to allow actions to be taken before a service impacting event occurs.

Hardware device monitors are either agent based or relay via a local agent to the RMM platform. This allows for not only the servers, laptops and workstations running the RMM argents but also smart devices on accessible networks, such as switches and routers to report back their health states to a central location and managed by our experienced team.

Signals from other platforms can also be ingested in the PSA platform to ensure there is a single view of all alerts. These could include other cloud platform, backup platforms or environmental platforms.

As all environments are different, we can amend baselines and setup specific monitors. These baselines are set initially when platforms are onboarded but reviewed constantly either during service review meetings or during the proactive, reoccurring problem management processes included within the support agreement.

A daily report of health checks can be agreed and configured, and this is shared with clients/ The contents of these reports can be agreed during the onboarding process and amended throughout the contract by raising a service request.

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Device Management

Management of all devices in scope is included in the service. This function is delivered as described in the monitoring and alerting service for all devices in scope of the agreement. Where the client has additional functionality, such as Microsoft Intune, the management of this platform is also included. The documentation of such a platform will either be completed during any onboarding session if present at that time or during deployment projects to implement such a system. Changes to this service will be included within the CAB meetings or via a service request.

Microsoft 365 Management

The day-to-day management and support of the Microsoft 365 environment is included within the agreement. Microsoft 365 Management refers to the administration and optimization of Microsoft 365 services across an organization. It encompasses:

User and License Management to add/remove users, assigning licenses, and monitoring usage. Maintaining security policies and compliance including the management of Intune if included in your license. Configuration and monitoring of Exchange Online, SharePoint, Teams, OneDrive, and endpoint security settings if included.

It also includes access to FinOps tools for cost optimization and compliance reporting. This management ensures productivity, security, and cost efficiency across the Microsoft 365 ecosystem

Central has a number of highly experienced and Microsoft qualified people we also have direct access to premium support from Microsoft due to our Microsoft Solution Partner designation. We also have access via our Microsoft vendor who also has access to higher levels with the Microsoft support domain to be called upon if required.

Asset Lifecycle Management

Asset management can be included in the agreement if required for all assets within scope. Procurement, configuration, deployment, maintenance and disposal can all be managed. Inventory reporting is available via our helpdesk platform or via a service request.

This service leverages the tools and "out of the box" experience provided with the Microsoft Intune platform if included within your license plan.

Incident and Request Management

Central’s Helpdesk service is at the heart of the operational delivery for all Incidents and requests. The service is designed to restore normal service operations as quickly as possible following an

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

unplanned interruption, while minimising business impact and serving any requests. The Helpdesk function will operate as described below:

a. Identification and Triage

   i. Identification of the request is initially split into 2 categories. Is the request a service incident, where something needs to be fixed and returned to BAU or is it a service request.

   ii. Incident triage is a critical process within ITIL Incident Management that involves assessing, categorizing, prioritizing, and assigning resources to resolve incidents efficiently. It ensures that the most urgent incidents are addressed first, preventing major disruptions and minimizing potential damage. The process starts with rapid detection and clear reporting, followed by assessment, categorization, prioritization, and documentation. This structured approach helps optimize response efforts and prevents minor issues from escalating.

   It is possible to include agreed knowledge articles, playbooks and workflows for specific actions on a per client basis. This flexibility allows us to tailor the service delivery to fore fill specific requirements ensuring security, compliance or service requirements are met.

iii. Automatically generated incidents generated from alerting and monitoring, will be logged within the same platform as all user based incidents and triaged.

iv. A service request refers to a user-initiated request for a predefined service or information. This can include requests for password resets, software installations, hardware requests, or access permissions. Service requests are generally routine, predefined, and repetitive in nature, aimed at fulfilling specific user needs or enabling access to certain IT services. Dependant on the nature of the request and the impact this request will be deferred to the Change Authorisation Board (CAB) for review.

b. Escalations and Resolutions

   i. Incident Escalations are handled as shown in the Helpdesk Workflow Diagram.

   ii. 1st Line service will perform the basic triage, identification and primary actions for any incident. Confirmation of repeatable conditions, log collection before reviewing knowledge articles to affect a fix. Use of the RMM tool, could be used in conjunction with other resources to collect logs or deliver a solution. If no resolution can be identified then escalating to either the 2nd Line team, customer or a Third Party Supplier/Vendor as per the service agreement.

   iii. 2nd Line service will continue from the 1st line process. Reviewing the actions taken, reviewing logs, the knowledge article and playbooks before reviewing the additional methods to affect a resolution or escalate to 3rd line.

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

iv. 3rd Line shall remain responsible for all 1st line and 2nd line support. Further advanced investigation by a product specialist and shall, where applicable escalate incidents to the supplier via its service desk to assist in the escalation of 3rd line support to a Third Party Supplier

v. Facilitation of, or engagement with 3rd Party suppliers is included to provide a cooperative approach to technical incident resolution.

vi. All updates and actions taken in pursuit of the resolution will be logged within the PSA platform. Each entry will include the time the action took place and is fully auditable

vii. All credentials used throughout the process will be store in and retrieved from the password management platform. In which all actions are fully audited

c. Resolutions

i. Client specific Playbooks and Knowledge base articles will be used to ensure prompt resolution. These can be reviewed in relevant account management meetings.

ii. Problem tickets will be managed on a weekly basis and where required included in the CAB, account reviews or escalated as appropriate to client for discussion.

iii. Change control is included in the service and can be held bi-weekly 30-minute sessions to address any service changes.

d. Feedback

i. Optional feedback from all client interactions is requested at the end of each incident or request to aid continually improve and review.

e. Reports and Measurement

i. All activities conducted within the PSA platform are logged to ensure measurements can be taken and audits conducted.

ii. As part of any service offering that would use the Helpdesk platform, regular account and service meetings would include a review of specific activities to help identify trends, opportunities for training or improvements in service encompassed in the specific support service agreement.

iii. Monthly analytics session which reviews consumption and performance can be included in the account management meetings. A "FinOps" toolset can be used as part of this process for the Microsoft Azure consumption.

iv. Depending on the contracted service level, problem management reports will also be generated and addressed.

Patch Management

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

The RMM agent used to support the monitoring and alerting service is also used to deliver our patching solution. This can deliver operating system patches for end user devices, both Microsoft Windows and Apple, alongside common 3rd party applications. Polices can be tailored to each environment to ensure appropriate patching and any interruption is kept to a predicable minimum, ensuring you are always compliant with your security governance policies.

Problem Management

Central's Problem Management service is part of its ITIL-aligned managed support offering and is designed to reduce recurring issues and improve overall service stability. The service focuses on identifying and addressing the root cause of recurring incidents, rather than just resolving individual tickets. This helps prevent future disruptions and supports continual service improvement.

Using a combination of automated workflows or manual actions, problem tickets are raised in the service platform for review and form part of the conversations in account reviews, change control and supporting the technology roadmap.

Change Control

Central's Change Control service ensures that all changes to IT systems and infrastructure are planned, assessed, and approved in a structured manner, reducing risk and maintaining service stability. Regular Change Control Meetings, weekly or bi-weekly sessions to review and approve changes.

Azure Management

Central's Azure Management service focuses on the administration, optimisation, and monitoring of Microsoft Azure environments to ensure stability, security, and cost efficiency. Including the use of Azure Cost Management tools and FinOps platforms to analyse spend, forecast usage, and prevent overspend through alerts and budgeting. Design, deploy and support services for Azure workloads can also be managed by our in-house teams.

Backup Alerting and Monitoring

Monitoring of the backup is included within the service for all in scope platforms. Any alerts generated are passed into the Central helpdesk function for appropriate review and remediation. All alerts are reported daily.

Backup as a Service

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Central's Backup as a Service provides a secure, offsite backup solution designed to protect critical data against loss, corruption, or disaster. It ensures compliance with best practices and offers resilience for business continuity. This service can be tailored to incorporate the individual elements or your environment and business requirements. From use our Central Cloud services to a blended solution included in place resources or other SaaS platforms to provide a comprehensive backup solution. This service is then monitored from the helpdesk platform with testing and recovery services available via our professional services team.

Disaster Recovery as a Service (DRaaS)

Central's DRaaS is designed to ensure business continuity and resilience by providing rapid recovery of critical systems in the event of outages, cyberattacks, or natural disasters. It combines cloud-based replication, orchestration, and managed services to minimise downtime and operational risk.

Utilising Central's private cloud datacentres alongside public cloud platforms such as Microsoft Azure Site Recovery (ASR) for flexibility and scalability Central can provide a complete solution. Including continuous replication of virtual machines and physical servers to secure offsite locations, ensuring RPOs are met and significantly reduced RTO for critical workloads.

With continual monitoring and regular, controlled enactment of the DR plan Central can validate recovery plans without impacting production systems.

Business Continuity Planning Support

Central's BCP Support ensures organisations can maintain critical operations during disruptions by providing planning, documentation, and proactive resilience measures. It is part of the wider Resilience and Recovery service portfolio. Leveraging the data collect from sources including the Annual Technology reports and initial onboarding and discovery exercises alongside your business and technology roadmaps Central can provide support and planning for your business continuity plan. Helping to ensure all systems are identified and included within your plan.

From designing out high risk resources to supporting the building of recovery plans, testing and enacting them, Central can call upon our inhouse teams to provide this function.

Managed Detection and Response for Endpoints

Central's Managed Detection and Response for Endpoints (MDR) service is a fully managed, 24/7 cyber security solution designed to protect your organisation against modern threats by combining advanced detection technologies with expert human analysis. It goes beyond traditional antivirus by delivering real-time monitoring, investigation, and response across endpoints, identities, and cloud environments.

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Providing continuous monitoring of endpoint activity to detect suspicious behaviour and advanced threats such as ransomware, fileless attacks, unauthorised remote access tools and even poor password hygiene on devices. With automated actions including isolating compromised devices to prevent lateral movement and helping to centralised antivirus policies, this platform helps protect your environment from the next level of threats.

The agent can be deployed with the use of the RMM tooling included in our support offering and all activities are logged within the helpdesk platform and reported on monthly.

ITDR (Identity Threat Detection and Response)

Working hand in hand with the MDR service, the ITDR function protects user accounts and credentials by detecting anomalies like suspicious Microsoft 365 logins, privilege escalations, and malicious inbox rules. With a UK-based Security Operations Centre operates 24/7, handling alert triage, investigation, and remediation so you don't have to sift through false positives. No agent is required for this function as it directly leverages the M365 platform.

SIEM (Security Information and Event Management)

In addition to the endpoint devices and the user identities Central can also offer protection for the other items in your environment. Aggregating and analyses logs across your IT environment to identify patterns and indicators of compromise, enabling proactive threat hunting. A local collector agent is required for this function.

User Training and Awareness

Central can offer Security Awareness Training as part of its services, helping organisations combat social engineering and phishing threats by building a strong security culture. Using one of the world's largest platforms for security awareness and simulated phishing, trusted by thousands of organisations globally.

The platform includes training content covering phishing, social engineering, and compliance topics. It then deploys automated and targeted phishing tests to measure user susceptibility and reinforce learning. Risk scoring and reporting is then available and delivered to you via regular reports and can be discussed during service and account management reviews.

Helping to reduce human risk and strengthen security culture. Empowering employees to act as a "human firewall" and delivering regulatory compliance and continuous improvement

Cyber Essentials/Cyber Essentials Plus as a Service

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Central delivers Cyber Essentials as a Service (CEaaS) and Cyber Essentials Plus as part of its Central Cyber Secure managed security offering. These services help organisations achieve and maintain UK Government-backed Cyber Essentials certification, demonstrating robust security controls and compliance with recognised standards.

Helping with every step of the process and ensuring you understand each security baseline so you not only achieve the certification level to unlock new markets and secure your business but going further so you can adopt these practices across the business and stay safe and compliant.

The service allows Central to work with you on a collaborative way to identify the scope, complete the questionnaire and be there to ensure that the vulnerability scans are managed in a seamless manner. Central is then there throughout the year to ensure compliance with the framework.

Patch Assurance and Vulnerability Management

Central's Patch Assurance and Vulnerability Management is a fully managed service designed to keep your IT environment secure, compliant, and resilient. It combines automated patch deployment with continuous vulnerability scanning and remediation, ensuring systems remain protected against emerging threats and aligned with industry standards such as IASME Cyber Essentials Plus.

Building the service offered as the Patch Management Service, the policies are tightened to ensure deployment of patches are with certification compliance and then a vulnerability service is added to ensure there are no additional remediation required.

Depending on the environment and requirements a suitable vulnerability tool is used to assess and report on the environment. This can be completely managed by Central or co-managed utilising your services team. A complete report of patching, vulnerabilities and remediation is then available.

Professional Services Days

Along side the support services, Central can also provide access to our Professional Services team. A highly skilled team of technology architects and deployment experts to support you with technical changes outside of the support scope and to align your technology stack with your roadmap.

Professional service days can be purchased in blocks of days in advance to aid with quick deployment. Alternatively, they can be purchased on an ad hoc basis as the business need arises.

Booking of the Professional Services Team can either be made via a service request directly to the service team, during a CAB or service meeting or by contacting you're account manager.

Onsite Technical Attendance

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Central offers Onsite Technical Attendance as part of its managed service portfolio, designed to provide flexible, ITIL-aligned support when remote resolution isn't sufficient or when clients need additional technical presence.

Available as ad hoc visits, pre-arranged regular attendance (e.g., weekly), or permanent onsite staff. Can supplement internal teams for project deployments or act as an onsite presence for organisations without dedicated IT staff.

Booking of the Professional Services Team can either be made via a service request directly to the service team, during service meeting or by contacting you're account manager.

Onboarding and Adoption

Central's Onboarding Service ensures a seamless transition into managed support by delivering a structured onboarding project ahead of the formal contract start date. The goal is to integrate Central's systems and processes with your environment without disrupting business operations.

Starting with open discussions and regular onboarding meetings with key stakeholders to track progress, resolve issues, and ensure alignment. Communication plans and milestones are agreed upfront along with key objectives around authorisations and security protocols.

This leads to a comprehensive review of your existing infrastructure, including servers, networking, backups, and security protocols. This establishes a baseline for support and compliance. Moving to integration of Central's ITIL-aligned Service Desk and Remote Monitoring & Management (RMM) platform across all endpoints, servers, and network devices enables proactive monitoring, patching, and streamlined support. With training sessions for internal IT teams and end users on how to log tickets, access the knowledge base, and use the support portal effectively.

All this concludes with detailed onboarding report documenting infrastructure, escalation paths, and support procedures. This serves as a reference for future projects and audits.

Annual Technology Report

Central's Annual Technology Report is a comprehensive review and health check of your organisation's IT infrastructure, designed to provide strategic insight, compliance assurance, and a roadmap for future improvements. It is delivered as part of Central's managed service offering.

Including detailed assessment of servers, networking, virtual environments, firewalls, endpoint protection, and backup systems. Verification of Microsoft 365, Azure, and other software licences to ensure compliance and cost optimisation. Evaluation of endpoint protection, web filtering, and cyber security measures, including recommendations for improvement. Review of backup strategies, DRaaS configurations, and failover capabilities to ensure business continuity. Concluding with strategic recommendations for upgrades, cloud adoption, and emerging technologies to support growth and efficiency.

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

The report is complied by our internal team who will know you and your business. So this isn't just an automated report but an in-depth dive into your technology stack and support by our knowledge of your business and goals.

Providing improved visibility and clear understanding of your IT estate and its alignment with best practices. Reducing risk, identifying and mitigation of vulnerabilities before they impact operations. With insights into licensing and resource usage to reduce unnecessary spend. All of which enables informed decisions for future technology investments.

Innovation and Automation Workshops

These workshops provide a strategic forum for senior stakeholders and technical teams to understand and implement innovations such as AI-driven automation, network optimisation, and process improvements. They aim to identify opportunities for transformation and align technology adoption with business objectives.

Central aligns these sessions with your business goals and provide a blend of inhouse expertise with vendors or technology creators. These sessions can be used for high level strategy, technical adoption and deployment or even as a group of likeminded peers reviewing some of the challenges facing the industry.

Booking of these sessions can done by contacting you're account manager.

Quarterly Technology Strategy Reviews

These reviews provide a strategic checkpoint every quarter, ensuring that your technology roadmap, infrastructure health, and security posture remain current and optimised. They form part of Central's advisory and account management services.

The review is completed by our own team of experts who know your systems and is delivered back in a report format, as the Annual Technology report is. this is supported by your account manager and inline with your technology roadmap.

Ticketing and Self-Service Portal

Central provides an ITIL-aligned ticketing and self-service portal as part of its managed support services. This portal is designed to streamline incident and service request management while empowering end users to resolve common issues independently.

Users can log incidents, service requests, project updates and changes via the web portal, email, or phone. The portal provides immediate ticket numbers and real-time status updates. The platform is equally at home as a repository from users to submit their queries or as a collaborative tool for co-managed environments, allowing for seamless escalation of tickets between teams, all with a single

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

pane of glass view allowing for easy reporting, auditing and insight into your environment and your users experiences.

Integrated Ticketing and Self-Service Portal

Allowing integration into your service team and further options around third party platform integration.

The ticketing platform can be taken a step further, allowing for your technical team to have access as a member of the Central technician team would. This offers a richer selection of features and allows your teams to act together as a team on a single platform and still have the ability to call upon Centrals resources when required.

This also opens up opportunities for integrations with third party platforms for incident reporting and integrated insight. This is commonly used with integrations such as Microsoft Entra, Microsoft Intune (for device insight) and a selection of RMM tools.

These options can all be discussed with your account manager.

Custom Workflows

From protocols and process you might require our teams to follow when engaging with your organization to specific technical steps and troubleshooting escalations you might need, we can facilitate it. All these can either be playbooks or knowledge articles within our platform or automated workflows with the ticketing platform, ensuring you get the expected output every time and quality is maintained.

These requirements can be captured and discussed during the onboarding phase and thereafter by submitting a request or simply discussion with your account manager.

Reporting

Central provides a range of monthly service reports to keep customers informed about operational performance, security posture, and service delivery. These reports are designed to offer transparency, actionable insights, and compliance assurance.

These reports are delivered either via automated email or via presentation during regular Account Management or service review meetings.

Service and Account Management

Central's support contracts include dedicated account and service management functions to ensure proactive governance, transparency, and strategic alignment between IT services and business

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

objectives. These functions go beyond technical resolution, providing structured engagement and reporting throughout the contract lifecycle.

Your dedicated account manager will act as a primary point of contact for all non-incident related matters. They will have regular meetings with all key stakeholders and attend project meetings to help align your business goals to your own IT roadmap and Centrals contribution to that.

Supported by our service leaders to help with the reviews of incident and service request activities. Providing reporting on all elements of the service delivery team and their interactions.

Together, with your own team, we will ensure all the of support elements included in the scope of the contract are aligned to the purpose of driving improvement within your organisation.

Exclusions

Although we do endeavour to include as many complimentary services within any agreement to remove any barriers to support there are inevitably some items that, unless otherwise clearly stated within the agreement, will be excluded. This is not a comprehensive list, but it does include:

1. Any Professional services required to commit any changes to the environment are not included. This includes any Scopes of work required to commit the change.
2. Bespoke application support
3. Telephony platform support or any integrations
4. Replace of, or addition of any hardware, excluding items covered by the any hardware warranty for assets included in the support agreement.
5. Any equipment which Central reasonably considers to be end of life, out of manufactures support, beyond repair, for which consumables, spare parts, drivers or updates are not readily available or require essential maintenance
6. Recovery from or Investigation into any kind of cyber incident.
7. Application of vendor updates
8. Any work outside of normal working hours

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

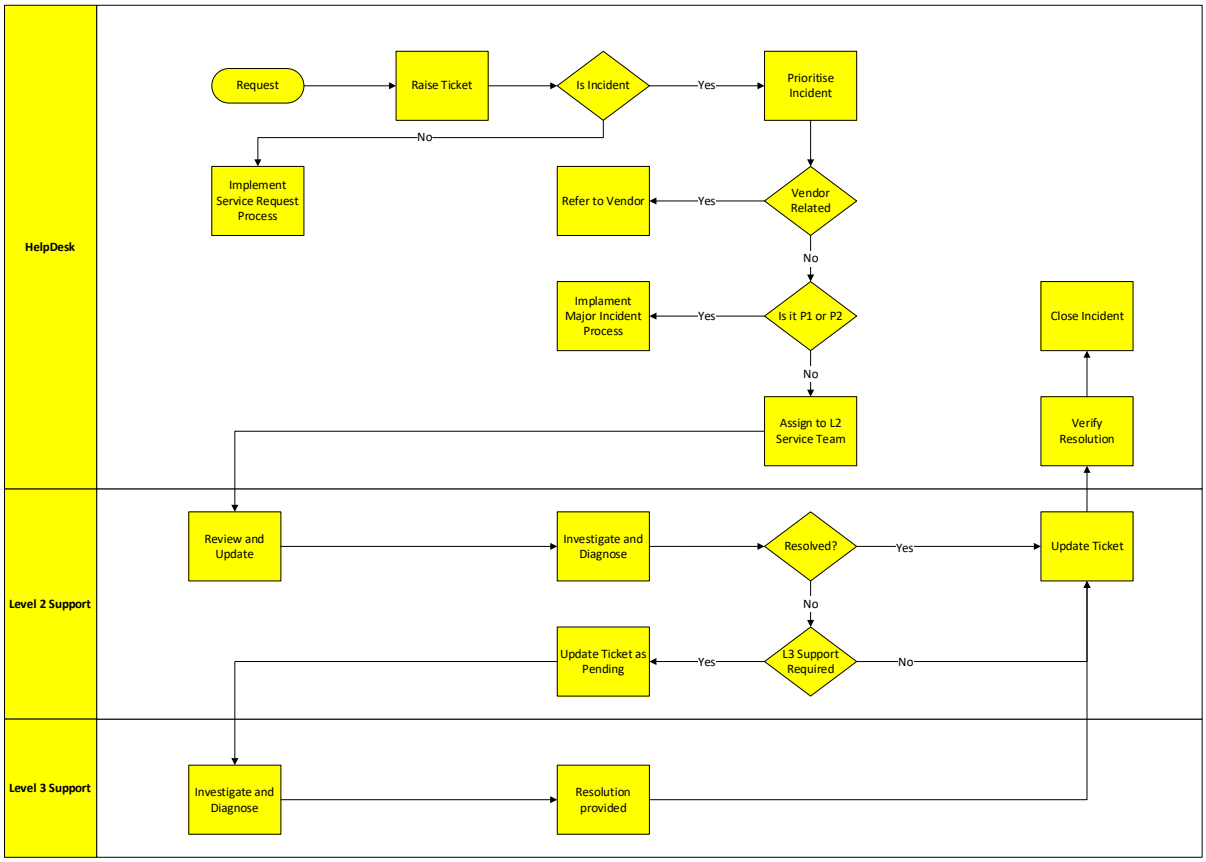
Terms of Engagement

This Service Engagement is governed by the Central Master Services Agreement and the associated support schedules:

- Central Master Services Agreement
- Central Support Patching and Monitoring Schedule

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

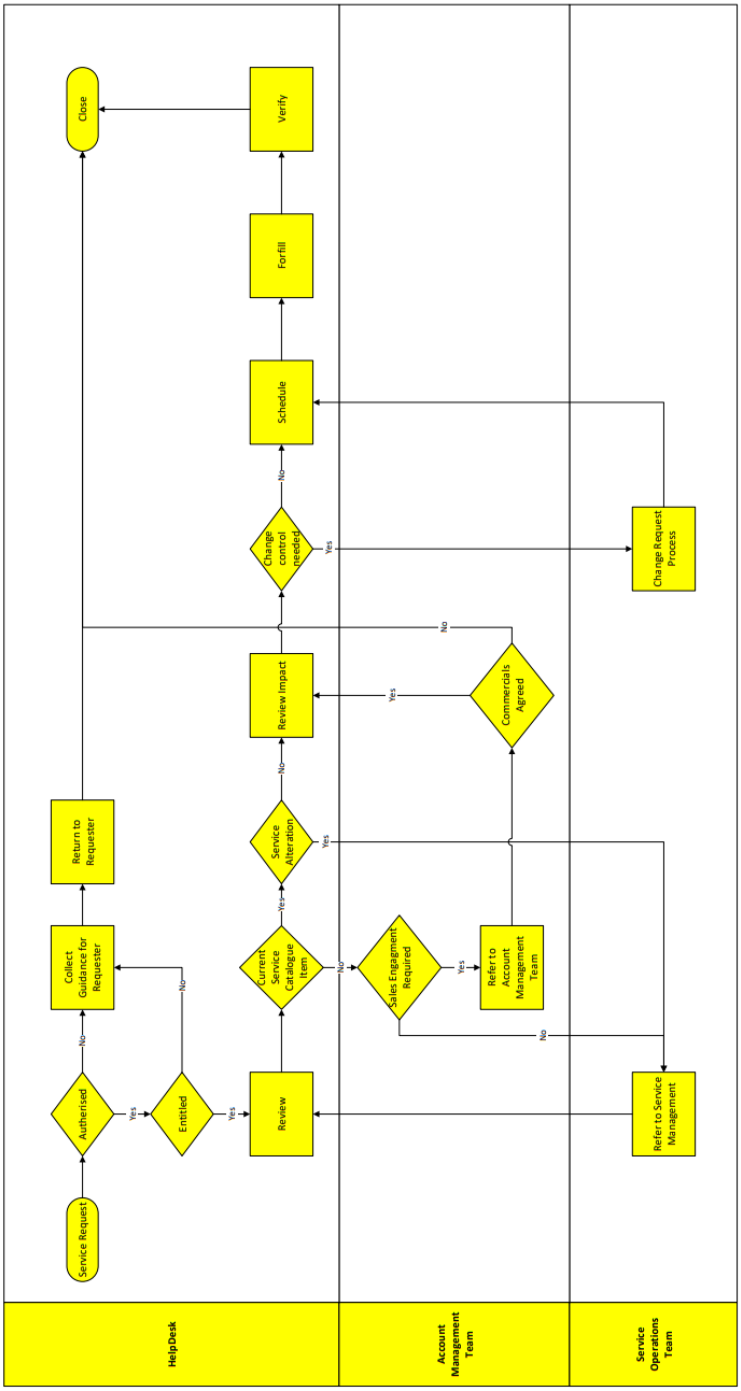
Appendix: Helpdesk Process



info@centralnetworks.co.uk
+44 (0)1706 747474
www.centralnetworks.co.uk

Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Appendix: Service Request Process



info@centralnetworks.co.uk
+44 (0)1706 747474
www.centralnetworks.co.uk