



Managed Wireless LAN Service Service Definition

G Cloud 15

Lot 2a – Infrastructure Software as a Service (iSaaS)

January 2026

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1. Service Overview	4
1.1 Service Overview	4
2. Service Description	5
2.1 Complementary Services	5
2.2 Service Design	5
2.3 Wireless Local Area Networks	5
2.4 Advanced Service Options	6
2.5 WLAN Internet Access and Communications Data	7
2.6 Licensing	8
2.7 Deployment	8
2.8 LAN Cabling	8
2.9 Management	8
2.10 Detection of Rogue Access Points	8
2.11 Monitoring / Alarms	8
2.12 Hardware Support	9
2.13 Standard Reports	9
2.14 Monitoring & Reporting Portal	9
2.15 Configuration Support and Change Requests	10
2.16 Performance Assurances	10
4. Associated Redcentric Services	12
5. Service Levels and Service Credits	13
5.1 Service Levels	13
5.2 Exclusions from Availability	13
5.3 Floor Service Level	13
5.4 Service Credits	13
6. Responsibilities and Accountabilities	14
6.1 High Level Redcentric Responsibilities	14
6.2 High Level Customer Responsibilities	14
7. Business Continuity and Disaster Recovery	15
7.1 Business Continuity	15
7.2 Disaster Recovery	15
8. Data Processing	17
8.1 Data Processing Scope	17
8.2 Data Storage and Encryption	17
8.3 Data Processing Decisions	17
8.4 Sub-processors	17
8.5 Customer Access to Data	17
8.6 Security Arrangements and Options	17
9. Exit Plan	18

10. Project management 19

11. Account management 21

12. Service management..... 22

13. Support Services 23

14. Information assurance 24

15. Professional services..... 25

16. Company profile 26

17. Why choose Redcentric? 27

1. Service Overview

1.1 Service Overview

The Redcentric Managed Wireless LAN Service (Managed WLAN Service) offers design, deployment, monitoring, support, and management of wireless LAN infrastructure deployed on Customer sites. The service utilises products from one of the leading Wireless LAN manufacturers. The service delivers enterprise features and uses centralised, cloud-based systems for provisioning, monitoring, and management. Engineers in Redcentric Service Management Centre (SMC) manage Customer WLAN environments undertaking administration tasks and resolving issues as necessary. The standard Service can be enhanced with additional optional functionality to offer enhanced Guest Internet Access for example. Charging for the Managed WLAN Service is based on a per access point, per month model.

2. Service Description

2.1 Complementary Services

Redcentric offers an extensive portfolio of services designed to meet the requirements of companies of all sizes. Specifically, Redcentric Managed Firewall Service, Managed LAN Switch Service, Internet Service, and connectivity portfolio are designed to complement the Managed WLAN Service.

2.2 Service Design

The Managed WLAN Service can accommodate a wide range of coverage, performance, and functionality requirements. Solution design is based on requirements of each individual customer site, and not a generic design.

2.2.1 Initial Design

A Radio Frequency (RF) coverage plan is produced using Customer provided location plans of the areas of the building(s) where WLAN coverage is required. The individual components required to deliver the Service including specific model(s) of Access Point (AP) and any centralised authentication infrastructure are derived from specific Customer requirements for each site.

The initial design is based on the following customer supplied information:

- Location floor plans
- Details of internal features (wall type)
- Anticipated user density
- Required services, e.g. Data, Voice, Guest Internet access etc.
- Security requirements including WLAN encryption and authentication methods
- Radio coverage and system redundancy requirements
- Details of Internet access where Redcentric is not providing Wide Area Network connectivity

External factors such as interference and building construction can affect the wireless coverage.

Customers can select optional site surveys which generally results in a design more likely to meet any Radio Frequency (RF) coverage requirements, and without a site survey the design is less likely to provide optimum coverage.

2.2.2 Design Guidelines

Redcentric produces initial desktop designs based on industry best practice by applying the following design principles by default

- For data only wireless, Redcentric will propose AP coverage overlap of 15% and no resilient AP visibility.
- For data only wireless where a level of resilience is required, Redcentric will propose AP coverage overlap of 15% per cell with visibility of 1 additional AP at -75dBm.
- For voice/video (e.g. real-time traffic), Redcentric will propose AP coverage overlap of 20% per cell with visibility of at least 2 AP's at -67dBm.

2.3 Wireless Local Area Networks

The standard Managed WLAN Service can support several Wireless LANs. Wireless LANs have many uses, two of the most common being 1) to extend the corporate wired LAN to support wireless end-user devices and 2) to provide visitors' Guest Internet access. A maximum of 8 Service Set

Identifiers (SSID's) can be configured. However, good design dictates that there should be as few as possible. Each SSID generally maps to a local VLAN on the wired LAN.

2.3.1 Corporate Wireless LAN

Connection to the Corporate LAN will be provided using a dedicated SSID which can be broadcast from all or a sub-set of the access points on the managed wireless network. Authentication and authorisation of corporate users and/or devices will be achieved using either:

- The Customer's existing RADIUS server and an authentication credential store such as the corporate Active Directory or a compatible LDAP compliant server. If the customer requires a RADIUS server to be supplied as part of the solution this can be provided at additional cost.
- A Redcentric supplied authentication server – please see section 2.4.1 below

2.3.2 Guest Internet Access Wireless LAN

The basic Managed WLAN Service enables the Customer to provide a basic Guest Internet access capability to its visitors, via a dedicated SSID. There are two alternative options:

2.3.2.1 Basic Guest services

If so, required by the Customer, the SSID may be configured as an 'open' SSID allowing a user to associate with this SSID with no requirement for a Pre-Shared Key.

On opening a web browser and attempting to access an Internet page the user will be re-directed to a 'captive portal' which will prompt the user to enter the pre-defined guest username and password. Once the user has input the correct details and accepted the applicable terms and conditions access to the Internet will then be permitted.

Redcentric will change the password on the Customer's behalf monthly (or less often if required) and inform the dedicated customer contact(s) of the new password.

2.3.2.3 Individual End User Authentication

As an alternative to using a generic guest user account, guest users can be authenticated against either a customer provided authentication server using the RADIUS protocol, or a Redcentric provided authentication server – please see paragraph 2.4.2 below.

Redcentric recommends the user authentication approach rather than a single shared username and password for all users since this will enable the customer to maintain greater oversight of the use of its service.

2.4 Advanced Service Options

The following services are optionally available to enhance the Standard Managed WLAN Service. Redcentric will provide you with details of applicable additional costs when designing the Service.

2.4.1 Enhanced Corporate Authentication Option

The enhanced corporate option provides the following features:

- Ability to apply relevant network permissions (E.g. VLAN assignment and/or firewall rules) based on the user's or workstation's group membership.
- Ability to apply Network Access Control (NAC) policies to devices. For example, this could ensure that devices connecting to the corporate WLAN meet anti-virus and patch management policies.

2.4.2 Enhanced Guest Option

The enhanced guest option provides the following features:

- Guest sponsorship. As part of the Guest login process, a web portal prompts guests to provide the email address of their visiting sponsor. The sponsor can grant or reject access to the Guest.
- Use of text messages to associate a mobile phone number with a user. Naturally a Short Message Service (SMS) gateway is required to achieve this, and SMS charges are applicable.
- Portal customisation. This allows customisation of the guest registration interfaces to provide full corporate branding. The Customer is required to provide Redcentric suitably formatted template(s).
- Guest portal access. This provides access to authorised users and allows them to review, configure, customise and monitor guest accounts (e.g. view guest activity and set the start date and/or end date of individual accounts)
- Multiple guest portals. Required when Customers have different Guest profiles, each to be treated differently.

2.4.3 Onboarding of Non-Corporate Devices Option

This option allows Customers to implement on boarding policies for non-corporate devices and control the level of access these devices have within the corporate network.

This option presents a dedicated WLAN (SSID) where non-corporate devices can connect. Authentication requests are passed to the Customer's corporate directory infrastructure using the method described in the standard service corporate access section above. Assuming access is granted, a digital certificate is made available for the device to accept. If that device is subsequently lost or stolen the certificate can be revoked to prevent that device gaining access to the corporate network.

To have a previously authorised device's certificate revoked, the customer should contact the Redcentric helpdesk with full details of the device (make, model and MAC address) and Redcentric will carry out the revocation on the Customer's behalf.

2.4.4 Internet Access Policy Enforcement – Managed Firewall Option

Standard design dictates that users connected to the corporate WLAN access the Internet through the same gateway (i.e. firewalls) as corporate devices on the wired network – this does not form part of the Managed WLAN Service.

Where users connected to the Guest WLAN access the Internet via Redcentric central infrastructure, a dedicated security gateway is required. For optimum functionality, Redcentric deploys next generation firewalls where the Customer does not wish to deploy their own Guest Internet firewall(s).

Redcentric next generation firewalls support content filtering, anti-virus, and intrusion detection functionality in addition to application-aware firewalling. Furthermore, models from one firewall manufacturer communicate with the wireless LAN infrastructure through Application Programming Interfaces (API) to provide unrivalled logging and reporting capability.

2.5 WLAN Internet Access and Communications Data

The Customer Corporate Wireless LAN and Guest Internet Access Wireless LAN services (together "WLAN Services") will be provided to end users by the Customer, and not by Redcentric (Redcentric will provide such services to the Customer as subcontractor). The WLAN Services will be branded accordingly, and basic branding will be set up during implementation of the services. Bespoke branding will be provided if the Customer chooses the portal customisation services, see paragraph 2.4.2.

The Customer will be responsible for all user management in relation to the WLAN Services, including (1) (unless otherwise agreed in writing) user authentication and (2) maintaining and supplying to government agencies etc. any records relating to the use of the WLAN Services as required by law from time to time.

The WLAN Services are set up in such a way that each end user must accept the Customer's end user licence agreement (EULA) before being able to access the service. The WLAN Services are provided with a simple and generic EULA between the Customer and the end user. The generic EULA will not be suitable for the Customer's business, and the Customer must amend the EULA to suit its own requirements (as explained in, and subject to, the legal agreement between Redcentric and the Customer).

2.6 Licensing

All subscription and licensing costs required to deliver the basic and, when chosen, optional functionality are included in the Charges for the Managed WLAN Service. The number of licences incorporated into the design for the basic Service and any optional features form part of the contract between Redcentric and the Customer for the provision of the Services. If additional licences are required for any reason (e.g. to resolve issues relating to higher-than-expected user or guest count), additional one-off and/or recurring Charges (at Redcentric standard rates at the relevant time) may be applicable.

2.7 Deployment

Deployment of the Redcentric Managed WLAN Service is simplified thanks to Redcentric centralised provisioning platform. Access Points added to the Customer's appropriately configured local and wide area networks will connect to Redcentric centralised provisioning platform and use a secure connection to pull down configuration details.

The Managed WLAN Service has been designed so that Customers can physically deploy / install APs using their own resource. Alternatively, Redcentric can optionally arrange for engineering resource to complete this task at an additional cost.

2.8 LAN Cabling

Charging for the basic service does not include any structured cabling checks, cable work or patching between the Customer's existing wired switch infrastructure and the location of each AP. Redcentric will undertake a general or detailed survey of existing structured cabling on request and provide a report on its suitability. Redcentric can arrange for cabling to be upgraded, repaired, corrected, extended, tidied, re-patched, labelled and replaced as required to ensure a customer's entire LAN is fit for purpose. This work is chargeable.

2.9 Management

Once deployed and commissioned, the Managed WLAN Service will be managed by Redcentric to ensure the wireless infrastructure is available and performs optimally. Management is provided by engineers in Redcentric SMC using a centralised management platform which connects to the WLAN infrastructure using secure tunnels.

2.10 Detection of Rogue Access Points

The Managed WLAN Service APs monitor the RF space for other APs advertising the defined SSIDs in the surrounding area. If one of the defined SSIDs is being broadcast by another AP in the area, the managed AP reports details of the adjacent AP back to the centralised management server. If the adjacent AP is not on the list of APs being managed, the management server raises a rogue AP alert. A ticket will be raised and Redcentric staff will contact the customer. Rogue APs are a potentially serious security issue, and the customer should deal with the rogue AP as quickly as possible.

2.11 Monitoring / Alarms

Under normal circumstances the Redcentric systems poll each access point every 5 minutes to confirm that it is available. This is in line with industry standard network management best practices. If an AP does not respond to several successive polls, an automatic alert is forwarded to the

Redcentric network fault management system. This automatically raises an incident, which is placed in the technical support queue. Technical support engineers investigate these incidents 24 hours a day, 365 days a year.

Customers can become aware of problems in the short window before the polling procedures verify a problem and issue an alert. Redcentric provides additional means for Customers to raise faults, i.e. via telephone, email, and the web portal.

Redcentric classifies problems according to severity. This allows the prioritisation of resource on issues that have the most impact on Customers' businesses. Further details of the classifications can be found in the Redcentric Customer Service Plan (CSP) which is available on request.

Redcentric is committed to continually improving and expanding its services, and to facilitate these improvements, it is necessary to carry out essential work from time to time. In accordance with Information Technology Infrastructure Library (ITIL) service management standards, these activities are carefully scheduled using an internal change control process; this gives Customers maximum visibility of any given change and thereby ensures that planning and implementation is carried out to minimise the effect on Customers using Redcentric services.

Maintenance windows and procedures for communicating emergency outages are detailed in the CSP.

As well as availability polls, information regarding other aspects of the service is retrieved from the various platforms. Redcentric sets alarm thresholds for these parameters and support staff act accordingly when alarms are received.

2.12 Hardware Support

If Redcentric Support Desk determine that an AP has developed a fault, Redcentric will arrange a replacement by the 'next business day'. Customers can choose an expedited option which offers a target hardware replacement timeframe of 4 hours from the point that Redcentric determines a replacement is required. This timeframe is not practical for certain remote UK locations and Redcentric will notify the Customer of alternative target timeframes for these locations. Naturally, expedited hardware replacement will not improve repair times for faults caused by anything else. The expedited option is incorporated into the monthly Service Charge and is applicable regardless of the number of times it is called upon.

2.13 Standard Reports

Standard pre-defined reports provide Customers useful summary information on the following aspects of their service – a sample report is available:

- Access Point Uptime
- Bandwidth Usage
- SSID Usage
- Client Session Report
- Failed Authentications
- Rogues Aps

Customers can use the monitoring / reporting portal to tailor these reports or produce other specific reports and access other useful information.

2.14 Monitoring & Reporting Portal

As part of the establishment process Redcentric will provide the Customer access to management portal(s) for the Managed WLAN Service that provides real-time and historical information including the following:

- Access Point inventory and status
- Access point client connection details – active and historical
- Access Point utilisation
- Security events – e.g. rogue AP detection
- Visual radio frequency overview, heat map and floor plan coverage (Note: this is dependent on the Customer supplying floor plans and details of access points they physically deployed)

2.15 Configuration Support and Change Requests

The validation and consequential implementation of change requests will be performed Monday to Friday between 8 am and 6 pm, with a target completion time of 48 hours for routine changes. Emergency changes are prioritised accordingly, and performance targets are detailed in the Redcentric Customer Service Plan (CSP).

In accordance with the Redcentric change request procedure, all change requests must be submitted by a designated and authorised Customer technical contact. If the Redcentric engineer cannot validate the change requester against the authorised list, the engineer will place the change request on hold and attempt to contact one of the alternative authorised contacts. Redcentric must wait for the request to be ratified by a known authorised contact before proceeding with any change. It is therefore essential that Customers provide accurate and current contact information for their designated and authorised staff.

It is extremely easy to weaken network security by submitting a seemingly innocuous change request. Redcentric staff review change requests based only on the information they have available, and therefore Redcentric cannot take responsibility for weakness resulting from changes. If Redcentric support staff believe that a change request compromises the security of the Customer's network, Redcentric may ask the Customer to sign a disclaimer stating that they wish to go ahead regardless of the advice offered. In extreme cases, staff reserve the right to reject the change outright; for example, if the weakness could affect other Redcentric Customers.

2.16 Performance Assurances

Due to the nature of wireless networks where environmental conditions change constantly and it is not possible to control user density, any issues relating to RF interference and bandwidth congestion are beyond Redcentric control, e.g. coverage, throughput, bandwidth availability etc.).

2.17 Security arrangements and options

Redcentric core infrastructure and hosting locations comply with ISO27001 / ISO27002 information security standard and controls.

3. Onboarding and Offboarding

3.1 Onboarding

Redcentric offer a fully managed service with advice and guidance based on customer requirements for resiliency, cost, throughput capability requirements. We design solutions based on customer supplied floor plans, building infrastructure information and other factors to determine the best solution for each site environment

Our project and delivery teams fully implement the service, including configuration and testing, and work closely with customers to ensure the delivery of services to the required specifications.

3.2 Acceptance Criteria

The following Acceptance Criteria apply to the Managed WLAN Service:

- Confirm that a sample of devices can authenticate and connect to the Customer's corporate WLAN
- Confirm that a sample of devices can authenticate and connect to the Guest WLAN(s)
- Confirm that Customer can access administration portal(s)

3.3 Offboarding

Redcentric project, delivery and support teams will work closely with customers to gracefully close-down any services at their contract end and, if required, assist in any transition or migratory tasks with the customer and any new service provider

4. Associated Redcentric Services

The table below provides details of other compatible services with DDoS Mitigation Services available from Redcentric via on G-Cloud 15.

Service Name	Service Summary
Network as a Service	Network as a Service provides a secure internal / external network connection. It meets compliance standards and various Redcentric services such as internet and security can be overlayed over this single connection into the Redcentric Network.
Managed Firewall Service	Managed Firewall Service The service is delivered on virtual firewalls on a shared platform or on one or more dedicated hardware firewall appliances. The firewall control traffic between devices on different networks and provides perimeter protection. The firewall is configured by our staff to meet customer's requirements. Firewalls are monitored for alerts.
Managed LAN Switch Services	Managed LAN Switch Services provides an Ethernet LAN switch located on a customer site to provide connectivity between compatible, hard-wired Ethernet LAN devices. Typically, the switch would be the central connectivity point for PCs, Internet Protocol (IP) phones, servers, printers etc.
Managed SD WAN Service	Managed SD WAN Service is designed to complement traditional private IP-VPN networks. It allows customers to make optimum use of the available bandwidth at sites, and to supplement private connections with cellular, low-cost Internet and other links. Application visibility, control and performance can be enhanced, delivering greater efficiency and user satisfaction.
Managed Wireless LAN Service	Managed Wireless LAN Service offers design, deployment, monitoring, support, and management of wireless LAN infrastructure deployed on Customer sites. The service uses products from leading Wireless LAN manufacturers. The service delivers enterprise features and uses local or cloud-based systems for provisioning, monitoring, and management.
Meraki Connectivity and Security	Meraki Connectivity and Security. Meraki's range of connectivity and security devices are proving to be popular due to the market leading traffic visibility and diagnostic capabilities, also the scalability and ease of management using the cloud-based management portal. Redcentric Meraki service provides the design, deployment and ongoing support of Meraki's connectivity and security devices.
Secure Remote Access Service	Secure Remote Access Service offers a robust, scalable, flexible, and secure way for remote users to access information and business applications whilst away from their usual work location. Software on the user's device communicates with the remote access platform across any Internet connection and a secure tunnel is established.
Two Factor Authentication	Two Factor Authentication (2FA) service offers a robust, flexible, and secure way to authenticate user connection requests to network devices. The 2FA service can be deployed on both Customer Management and Redcentric managed network devices. The 2FA service offers a more secure and scalable alternative to static passwords.
Wireless Guest Access	Wireless Guest Access is an analytics and marketing service provided by our partners Purple. Redcentric resells, integrates, and supports the service. Used with wireless services to provide guest Wi-Fi experience, and venue owners valuable information on their customers and visitors, focused marketing communication and assists in the compliance implications associated.

5. Service Levels and Service Credits

5.1 Service Levels

The Service Level applicable to the Managed Wireless LAN Service is as follows:

Service Level: Availability of the Service at each individual Access Point	Measurement Period: Month
Service Level	Not less than 99.5% Availability

5.2 Exclusions from Availability

In calculating Availability, in addition to the exclusions listed within the General Terms of the Redcentric G Cloud 15 Supplier Terms the following shall be excluded:

- Failure of connectivity to the Customer site which prevents Redcentric from measuring Availability
- Inability of the Customer's LAN to connect to Redcentric remote platform due to a failure of WAN connectivity and/or any other cause that is not part of any Services being supplied by Redcentric
- Unavailability due to throughput (load) exceeding initial documented requirements
- Unavailability due to onsite power, cabling, or local network issues
- Malicious attempts to disrupt service such as wireless jamming, Denial of Service etc.

5.3 Floor Service Level

The Floor Service Level applicable to the Managed WLAN Service in respect of Availability shall be 85% per Access Point in any given Month - i.e. each Access Point has its own Availability Service Level and its own Floor Service Level.

5.4 Service Credits

The Service Credits applicable to the Managed WLAN Service shall be calculated as follows:

For each Access Point where availability is < 99.5% % in the relevant month, a Service Credit may be claimed according to the table below. The maximum value of Service Credits in any Month shall be a sum equal to half the Charges which would have been payable in respect of the aggregate of all Access Points in that Month had Redcentric provided the Managed WLAN Service in accordance with the applicable Service Levels.

In the following table:

“≥” means “greater than or equal to” and

“<” means “less than”

“MS” means the average Charge payable for an Access Point in respect of the WLAN Service for the same month.

Service Availability	Service Credits
≥ 99.5%	None
≥ 99.5% but < 99.0%	5% of MS
≥ 99.0% but < 96.5%	15% of MS
≥ 96.5%	20% of MS

6. Responsibilities and Accountabilities

6.1 High Level Redcentric Responsibilities

Redcentric is responsible for the following aspects:

- Solution design based on information and requirements provided by the customer
- Configuration of the centralised management, reporting, etc. components
- General upkeep of the platform including hardware and software upgrades
- Ongoing support of Customer-specific WLAN configuration including advice and implementation of minor changes
- Arranging replacement of faulty hardware

6.2 High Level Customer Responsibilities

The Customer is responsible for all other aspects including but not limited to:

- Providing Redcentric with the Customer's detailed coverage, functional and other requirements
- Providing Redcentric with the technical details required for the design. E.g. WLAN IP address ranges, SSID names, VLAN assignments, local DNS servers, DHCP scopes and options etc.
- Providing Redcentric with the Customer's branding template and Acceptable Use Policy (AUP) for Guest portal
- Providing Redcentric with suitable digital security certificate(s) as required – this is commonly a wild-card certificate
- Configuration of DNS to match the fully qualified domain name(s) of any required digital certificate(s)
- Install and connect access points unless Redcentric installation option is chosen
- Ensuring LAN is configured correctly and is fit for purpose, unless Redcentric Managed LAN switch option is chosen
- Ensuring suitable cabling is in place to connect access points to the wired LAN, unless Redcentric LAN cabling option is chosen
- Undertaking any design changes required after initial deployment
- Unless otherwise agreed with Redcentric, end user authentication, including supplying and maintaining an authentication platform being a RADIUS server and an authentication credential store such as the corporate Active Directory, or a compatible LDAP compliant server
- Meeting any compliance requirements associated with offering a public Internet service to guests
- Arranging and allowing access to site facilities at agreed times and for an appropriate window of time for the installation of any equipment related to the delivery of the service
- Completion of any required site risk assessment information prior to engineer site visits

7. Business Continuity and Disaster Recovery

7.1 Business Continuity

Redcentric under its ISO22301:2019 Business Continuity certification, operates and maintains a robust Business Continuity Management System (BCMS). The BCMS scope includes;

- Data Centers
- Managed Services
- ICT technologies and systems
- Staff and business functions

and is externally assessed by the BSI annually to ensure continued effectiveness in line with BSI published standards.

Our Business Continuity Policy Plan (BCP) is fully supported by the Board and is designed to enable a return to normal operations in the shortest practical time, with minimum disruption. The primary objective is to restore and deliver continuity of key services in the event of a critical incident.

Our overall Business Continuity strategy is to provide resilience for all systems that support critical processes, by having data backed up to alternative Data Centers, or dual site services configured as active-active.

We use the same cloud backup service (Acronis BaaS) for our own IT and services as we do for our customers, ensuring fully secure, encrypted data is available off-site when needed. Departments and services are required to test backup and restore annually.

Testing

Our BCP is routinely tested annually, and Redcentric is a provider of critical services to the NHS (Peering Exchange and Consumer Network Service Provider), is independently witnessed by a member of NHS England.

Disaster Recovery plans underpinning the BCP have been developed for each Department and Service, and these are externally audited and tested annually.

Network resilience

Our network has been designed and engineered to deliver highly available, stable connectivity to maintain business access to critical applications. To maximise resilience, multiple carriers provide core connectivity and routing, and switching devices are used by market leaders in Cisco Systems. The network design and build are geographically resilient, providing a minimum of 99.99% availability (to resilient end points).

The Redcentric highly resilient, high-capacity core has connections to several carriers providing multiple options for our internal business operations and critical services, and customers wishing to access cloud services, applications, and data:

- Geographically resilient connectivity to multiple tier-1 Internet transit providers and Internet exchanges.
- Geographically resilient connectivity directly into the inner core of the HSCN network.
- Core network engineered to withstand multiple concurrent failures and to re-route around a failed transit path in under a second.

7.2 Disaster Recovery

Wireless LAN management platforms are resilient across multiple geographically diverse locations and thus disaster recovery is automatically built into the service, however, the management platforms

do not, in and of themselves, limit the functionality of the service. In the event that management platforms become unreachable, the immediate functionality of the service is not affected.

In terms of wireless LAN access points, we recommend that customers take a pragmatic approach to the deployment of access points in any location and recommend that any deployment includes additional access points to provide wireless coverage if a single device becomes unserviceable. In the event of service failure, our support teams work closely with the customer to replace supported equipment in a timely manner.

8. Data Processing

8.1 Data Processing Scope

The Managed Wireless LAN Service delivers the transport of Ethernet packets between devices and does not involve any storage or backing up of data.

8.2 Data Storage and Encryption

Redcentric configures equipment to encrypt Wireless LAN traffic according to Customer requirements.

Redcentric Managed Wireless LAN platform captures standard information about traffic over the platform, including the MAC addresses of connecting devices, username, at which site and access point the connection took place, and for how long. This traffic data does not enable Redcentric to identify any individual and is retained to meet the Customer's needs in the management of the platform. As part of the standard configuration most traffic data is retained for up to a year and then deleted. Many of the data retention periods are configurable to meet the Customer's requirements and instructions (subject only to statutory data retention requirements), and these instructions can be dealt with as part of the initial implementation or subsequently.

Redcentric does not capture, inspect, analyse, store or share the customer's traffic/data under normal circumstances.

Under certain circumstances, when managing a support ticket, Redcentric may capture, inspect, analyse and/or store a small sample of the customer's traffic to investigate and diagnose a very specific problem, e.g. to help resolve a problem relating to packet corruption. Such diagnosis would involve the examination of a small sample of packets.

8.3 Data Processing Decisions

Redcentric does not make any data processing decisions in relation to the Managed Wireless LAN Switch Service. Any processing of data over Customer systems when using the Managed Wireless LAN Switch Service for transit is instigated, configured, and managed by the Customer.

Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Managed Wireless LAN Switch Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

8.4 Sub-processors

Except for physical deployment, no third parties are involved in delivering the Managed Wireless LAN Service, and there are no sub-processors appointed by Redcentric.

8.5 Customer Access to Data

The Customer controls its own platforms which use the Managed Wireless LAN Service to carry data, and the Customer therefore has full access to its own data.

8.6 Security Arrangements and Options

Redcentric core infrastructure and hosting locations comply with ISO27001 / ISO27002 information security standard and controls.

Managed Wireless LAN devices are located at Customer locations/sites. It is the Customer's responsibility to ensure physical security at such locations/sites meets its needs.

9. Exit Plan

Upon expiration of the Contract where the customer chooses not to renew with Redcentric, the steps set out in paragraph 3.3 will apply.

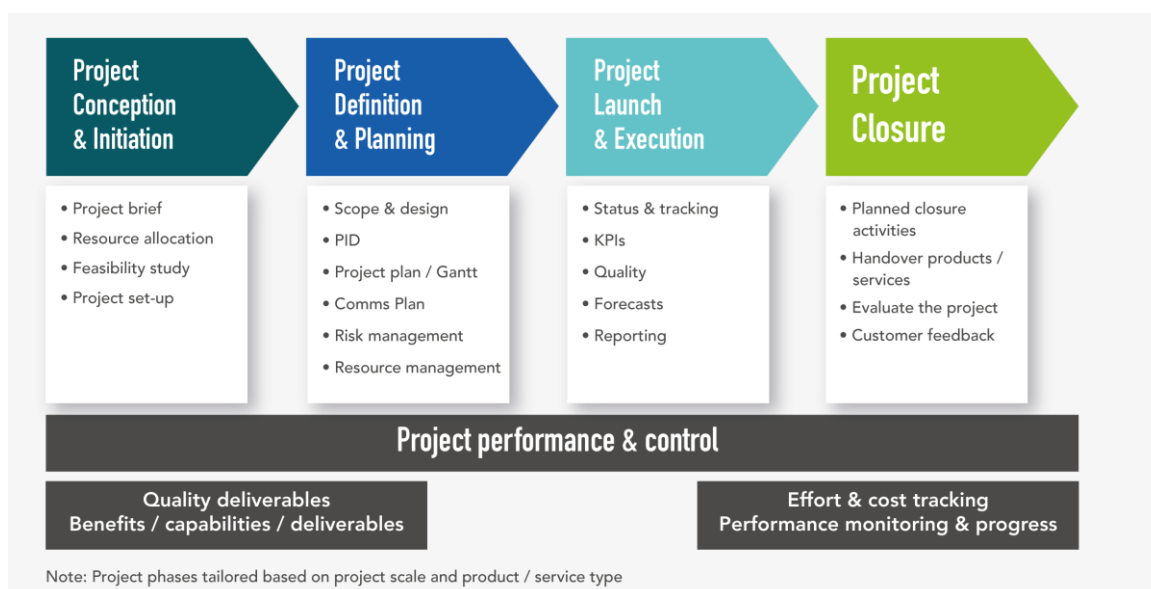
10. Project management

We understand you need to be confident we can deliver projects successfully and without risk to you or your customers. We know collaboration and communication with you is the key to successful project delivery, and the best way to ensure we can deliver the business value you expect from us.

Redcentric uses a hybrid project approach based on PRINCE2 and Waterfall methodologies, that is strengthened by ITIL project best practise. Our approach has been honed to foster a close working relationship between you and the dedicated project team that will be responsible for the onboarding of your new services.

The 4 phased approach that will steer your project delivery is:

- **Phase 1 – Conception and initiation**
- **Phase 2 – Definition and planning**
- **Phase 3 – Execution**
- **Phase 4 – Handover and closure**



We recognise the importance of making sure your project and programme of work is delivered on time and meet your quality and cost considerations. Our highly skilled team of project managers have years of project management and solutions expertise which enables us to provide you a clear understanding of when your solutions will be delivered in preparation for a seamless handover into live service.

You will benefit from our experience of managing a very broad spectrum of complex projects across our range of solutions for customers in a variety of sectors including highly sensitive sectors such as healthcare where disruption to BAU might result in a risk-to-life, or commercial sectors for example, retail or legal, where any disruption would have a significant impact on operational or commercial outcomes for the customer.

To meet your individual needs, we understand we need to be flexible to ensure we can deliver results quickly and with the expected outcome for the project. To achieve this, we will work closely with you to understand your needs and learn how issues impact your business. This will provide a clear insight into working together to resolve any challenges.

The main advantage of our meticulous approach is the handover process at each stage of the project. Risk is a key part of the agenda, which in turn promotes the continuity of risks and the identification of assumptions, issues, and dependencies. This early and continuous detection of risk means we can promptly and effectively mitigate any challenges as early as possible.

Quality assurance processes are embedded throughout the delivery lifecycle, underpinned by our ISO 9001, 14001, 20000, 22301 and 27001 certifications and supported by our centralised programme management office.

The project toolbox

We will use a suite of project tools designed to ensure your project delivery is seamless, transparent, managed effectively, and delivered to your agreed specification. Each device has been refined over time based on our experience and as our knowledge evolves with the introduction of new technologies.

- Project initiation document to develop a detailed scope of your requirements
- Comprehensive project plan to refine the delivery approach
- High level solution design
- Low level solution design
- RAID Log to identify, control and govern project risks
- Site audit report to help identify issues and challenges at each project location

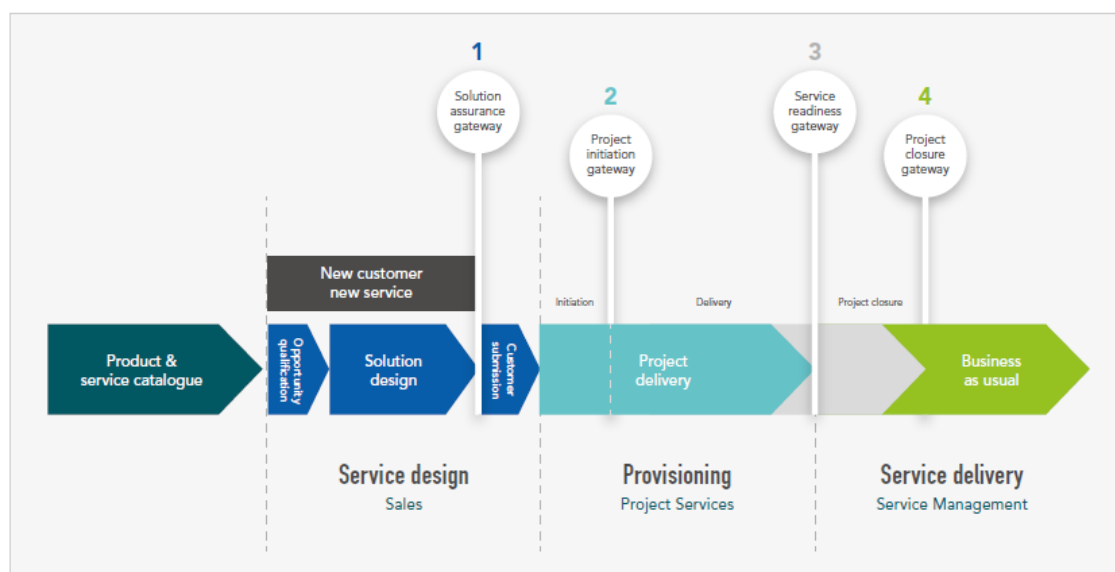
- Test plan to minimise disruption to your business operations
- Communications plan that defines what information to share and with whom
- Site implementation tracker to record the migration progress
- Weekly highlight report providing project updates
- Customer Service Pack
- UAT Test Report – per site (Word)
- Project Closure Report (Word)

Transition management

It is important to Redcentric that you experience a seamless and smooth transition into your service management team. With an established and proven approach to transitioning customers from solution design, through to projects and into your support team. Redcentric are confident you will feel supported and comfortable for the project team to step back, to let the service management team take over.

Using an effective project delivery approach throughout your transition journey, will ensure:

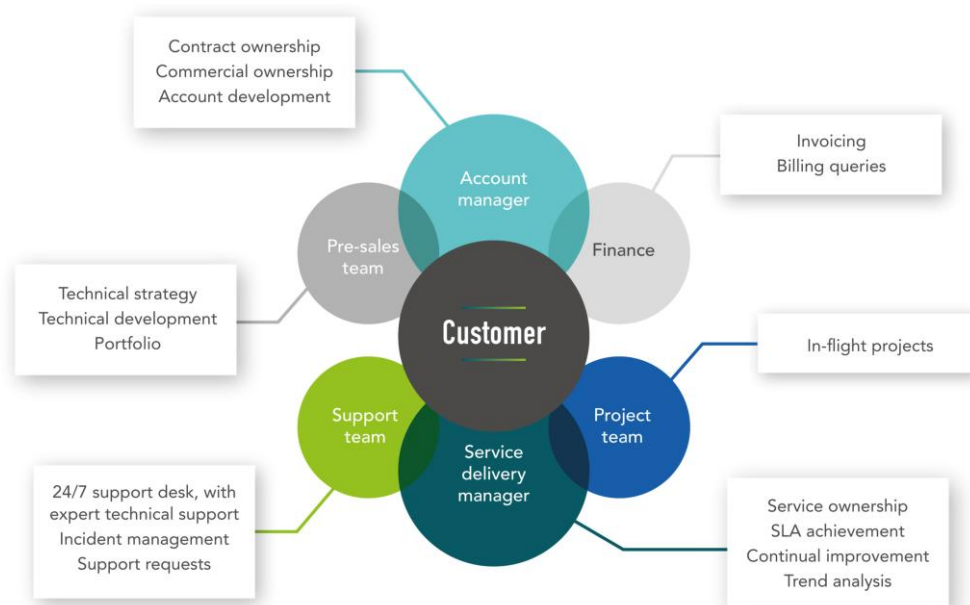
- Technical delivery is achieved on time and to specification
- The support model is fit for purpose and available at service commencement
- You will experience a 'soft landing' with minimal disruption to service.



With 30 years of track record of delivering projects, Redcentric is knowledge and approach to mitigating risk during the project transition phase is based on experience. Their mature and proven approach is employed as a standard risk management framework which flows from initial bid stage through to project delivery, and into live service.

11. Account management

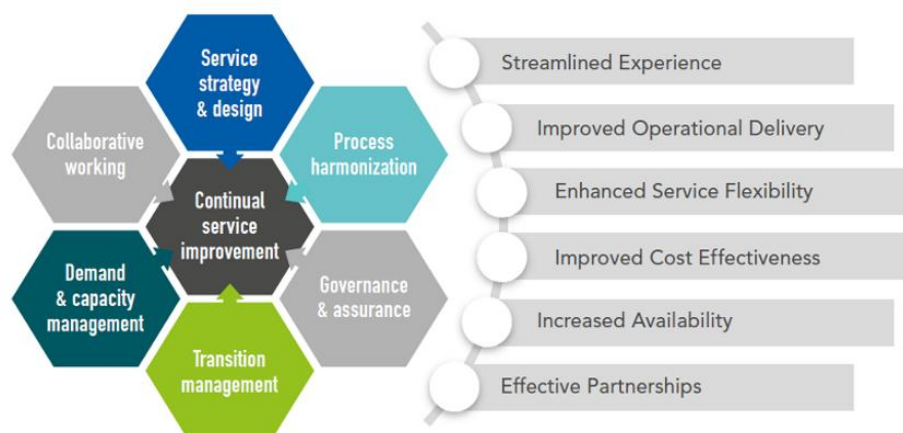
We appreciate the nature of your business demands an exceptional service. We recognise you need to be supported by a team who are not only competent and highly skilled, but also passionate about delivering the right outcome, every time. In our experience, this is achieved by aligning our expertise from the very beginning to create a single, cohesive, and focused team.



Your Account Manager will build an understanding of your current and long-term strategy and ensure that the wider Redcentric team understands your needs. They are responsible for the day-to-day commercial relationship between the customer and Redcentric. Our aim is to develop a long-standing partnership with you.

Sharing Technology advancements with you

A key role of your Redcentric account manager is to understand your business and to keep you proactively informed on the technology and industry developments that may be of strategic benefit to you. As part of your monthly service reviews, we will discuss our product and services roadmap and where required involve our technical design resources to better understand your requirement and provide guidance.



Our technology roadmap review forms part of the service delivery programme. Our aim is to ensure you are fully informed of the wider developments that we are planning to introduce and allow us to discuss any requirements you would like us to consider for the future.

Working in partnership to drive continuous improvement.

We fully embrace the continuous service improvement and will work with you to develop a continuous service improvement plan (CSIP). At the simplest level your CSIP will act as a way of prioritising and tracking minor improvement initiatives such as tweaking process to better suit your need but is equally used to drive technology enhancements and innovations to align evolving business requirements, including technology refresh, changes, and upgrades throughout the contract period.

12. Service management

Redcentric will provide a centralised service management model for all services we deliver to you. Our proven model will ensure you receive service management and support services that is easily accessible and effective.

Our mature processes are based on the ITIL framework, fully supported by Gartner-referenced service management tools and process automation which ensures you receive a best-in-class user experience.

The proposed solution is inclusive of our support and account management service, which include:

- Genuine 24/7/365 service desk which is manned, monitored and maintained using as mature ITSM tool
- Best-in-class secure management and monitoring tools, designed to ITIL guidelines.

Our service is underpinned by comprehensive, yet agile, documented processes that include major incident management. We have recently introduced enhanced SLAs within our support services, this means we will respond to you quicker and we are committing to faster fix times.

Service Reviews are an opportunity for us to collaboratively evaluate service performance and ensure it is effective and aligned to your needs. The service reviews seek to understand how we can work in partnership with you and your teams and to identify how we can improve performance. We work proactively to propose solutions to problems and suggest the best way to resolve any issues.



What happens at the monthly service review?

- Review service delivery using performance data and provide this in a graphical format.
- Analyse support tickets to identify patterns that indicate we need to explore further to identify the root cause.
- Review service availability, service exceptions, significant incidents, and related trends.
- Build operational relationships between our customers and the wider Redcentric team.
- Seek to align internal resources within Redcentric to ensure effective service delivery.
- Identify areas for improvement and include them in the service improvement plan.
- Seek your input on how we can evolve our services to suit your future objectives.
- Share our vision to demonstrate how we can support your future strategic aims.
- Create and hold formal records in the Redcentric document management system.

The monthly service pack provides a basis for discussion. It can be tailored to meet specific customer reporting needs as part of the onboarding process or within the lifetime of the contract. As standard, we provide a service pack that includes up to 12 months of data extracted from the support system and service monitoring systems. We analyse current and previous months' performance and identify any trends.

We operate a Service Management System which meets the requirements of ISO/IEC 20000, which means we have a tried and trusted model for service delivery that provides a consistent approach.

13. Support Services

We understand that our customers trust the Redcentric team to ensure that our services meet your needs. Our relationship with our customers goes beyond just complying with contractual SLAs and meeting industry standards.



We seek to understand the importance of service delivery to your organisation and work with you to provide the support that leads to the rapid resolution of any issues.



We take a pro-active approach to supporting you so you can be sure that the services which your business relies on are in safe hands.



Our support operations meet the highest industry standards, and service management processes are based on the ITIL framework.



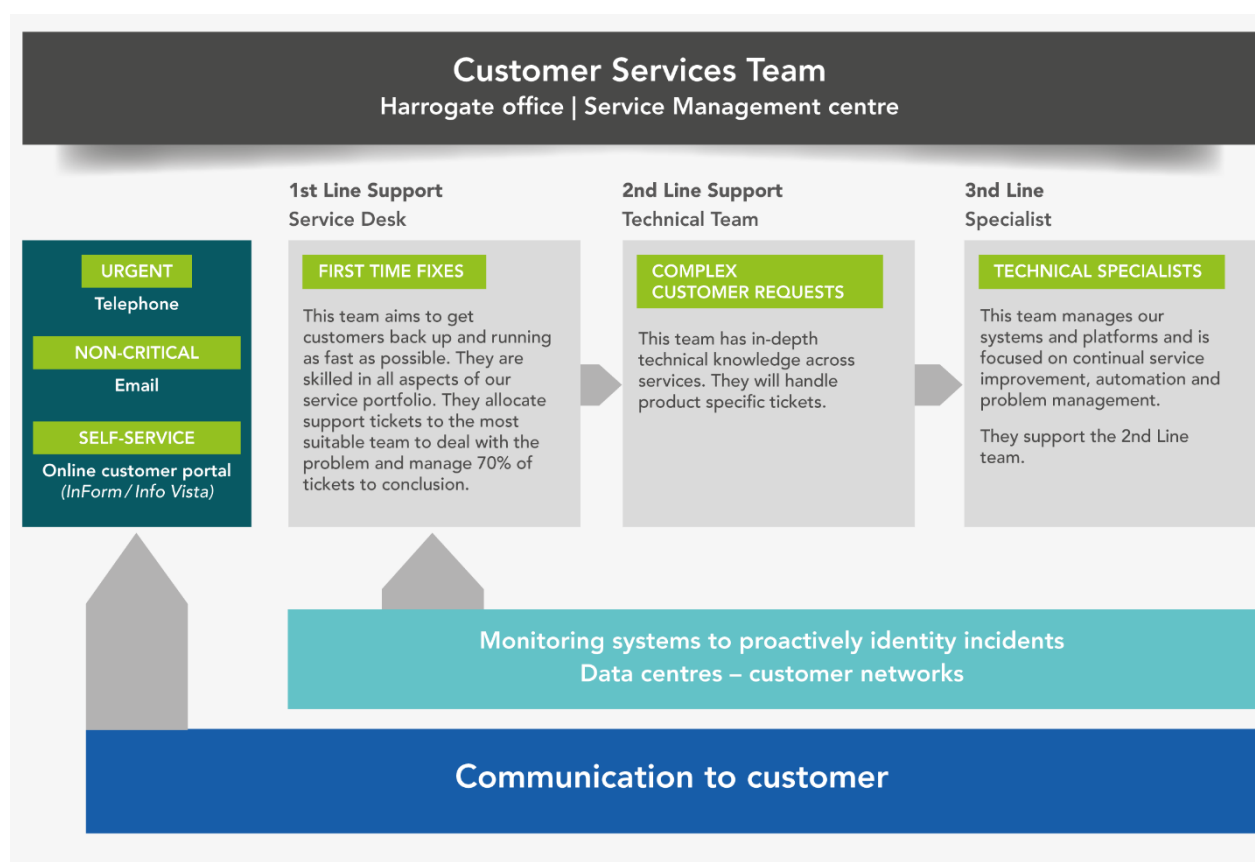
We have thoroughly documented the major incident and customer service plans, which detail how we operate in business-as-usual scenarios and during major incidents.



We use best-in-class secure monitoring tools to manage the services we provide to you actively. We use Gartner-referenced service management tools and process automation, which allow us to work smarter.

Our support function is structured to ensure fast resolution of incidents with timely escalation where appropriate.

The service journey you experience is important to us. Every interaction is monitored by our customer services team, who are highly experienced in handling customer interactions, and understand the importance gathering accurate and timely information to ensure the correct resources are allocated to reach a rapid conclusion.



Our incident management process has been engineered to be customer focused and designed to ITIL guidelines. We follow a proven process for incident management, with clear steps marked out for each team to ensure you are supported in the most effective and organised manner.

14. Information assurance

Certifications

Redcentric are ISO 20000-1 certified, demonstrating that we adhere to ITSM (IT Service Management) best practice, and ITIL (Information Technology Infrastructure Library) provides advice on ITSM best practice.

ITIL v4 is at the heart of Redcentric managed service operation and support. Redcentric believes that to deliver a high quality, professional service it is necessary to invest in training people, empowering them to be strong ambassadors of our service model.

Redcentric has provided managed services to the UK public and private sector for over 30 years. As a highly accredited business, we are proud of the standards and processes for which we are certified.

Our data centres and all supporting operations are fully UK Sovereign and are congruent with;

- The Government's Security Classification Policy ('Official-Sensitive')
- The Government's previous Protected Marking Scheme classification (BIL4 - Confidential)

Note – Redcentric can also support information and assets classified above the GSCP level of 'Official-Sensitive'.

ISO

- ISO 27001:2022 Information Security Certified
- ISO/IEC 27017:2015 Cloud Security Certified
- ISO/IEC 27018:2019 Personally Identifiable Information (PII)
- ISO 9001:2015 Quality Management Certified
- ISO22301:2019 Business Continuity Management
- ISO 14001:2015 Environmental Management System Certified
- ISO 20000-1:2018 IT Service Management System Certified

NHS standards

- Registered HSCN CNSP (Health and Social Care Network, Consumer Network Service Provider)
- DSPT (Data Security and Protection Toolkit) assessed as exceeding standards
- NHS Certified Commercial Aggregator
- NHS Business Partner
- Authorised to transmit, process and store Person Identifiable Data (PID)

- NHS England IGSoC Compliant Commercial Third Party (NACS code: YGMAP)
- NHS England accredited Service Provider (Network Access Agreement number: 0740).

HMG / other standards

- PCI-DSS Compliant for physical hosting and managed firewall services within our data centre locations
- Cyber Essentials Plus Certified
- Data Centres are externally certified to attest they have the necessary physical security measures to process HM Government 'Official-Sensitive' classified data
- Main data centres are certified as Police Assured Secure Facilities
- Full alignment with the Security Policy Framework
- All services are designed, built, implemented, and supported using all relevant and appropriate NCSC GPGs, Cabinet Office and NHS England standards

Networks Connectivity

- The Public Internet via Private or Public IP VPN
- The HSCN Peering Exchange
- PSTN
- PSN (Public Sector Network) certified as one of the few DNSPs (Direct Network Service Provider)
- PSN Gateway Access for both PSN-Assured and PSN-Protected
- JANET (Joint Academic Network)

Further information with regards to the Redcentric assurance and governance framework can be found within the Redcentric customer security pack which consist of the following documents:

- Cloud Security Principles (aligned with the NCSC 14 principles)
- Security Management Plan
- Security Statement
- Accreditations and Mappings (lists all business accreditations and relevant controls and standards utilised for Redcentric G-Cloud services)
- Security Control Framework

Copies are available under NDA upon request.

15. Professional services

The Redcentric Professional Services team is drawn from across the organisation, bringing together a unique mix of experience, know-how and talent to help deliver substantive value to its consulting assignments.

Strategists, designers, developers, technicians, engineers, analysts, security specialists and project managers from the worlds of infrastructure, networks, applications, communications, and mobile can come together to deliver expert, targeted, outcome-driven assistance where it's needed.

The common denominator in every professional services engagement is that we are responding to a specific client need. We provide tailored responses to your requests for assistance, whether that's for help of a strategic or tactical nature, short or long-term, on premises or off, single vendor or multi-vendor environment, in a lead role or in support.

Redcentric provide Professional Services using either our in-house team or approved third parties. Professional Services are not part of the service unless

so specified in the customer's order. Professional Services require a separate order or change control procedure.

Available services

- IT strategy.
- Project management.
- Change management.
- Design integration.
- Staging and installation.
- Integration design.
- Service migration.
- Optimisation and performance tuning.
- Physical lift and shifts.
- Audits and compliance.
- Application development.
- On premise and/or remote access support.

16. Company profile

Redcentric is a managed service provider, delivering highly available network, cloud and collaboration solutions that help public and private sector organisations succeed.

We provide:



Assured availability – Delivering highly available solutions that organisations can rely on to improve productivity and performance



Organisational Agility – Helping organisations to address operational, financial, and regulatory challenges at speed



Smarter Working – Enabling and empowering organisations to connect, communicate and collaborate

Our aim is to work in partnership with you to improve efficiencies, drive transformation and enhance the services you provide to your citizens, patients, students and tenants and our services are provided in line with the most stringent public sector standards.

We are here to support you, whether that be with traditional infrastructure or making the move and taking advantage of what the cloud and hybrid environments have to offer.

Today we can offer a rich end-to-end solution portfolio covering the full spectrum of cloud, network and collaboration designed and delivered by our own highly skilled teams from our privately owned, UK based multi-million-pound infrastructure.

Our ethos is one of collaboration; our aim is transformation: helping clients secure desired outcomes, substantive gains, and a measured route forward for the future.

Our assurance comes from a long track record across both the private and public sectors, characterised by deep domain expertise, continuous innovation, proactive management, and an enduring commitment to business improvement through better IT. We'd like to think that there are hundreds of organisations out there where Redcentric has already made a significant and lasting difference.

- Multiple wholly owned UK data centres
- Serving over 800 customers across the UK
- Health and Social Care Network approved CN-SP
- NHS Digital approved N3 Aggregator since 2014
- Accredited to connect and supply over Janet
- Authorised to process HM Government data marked 'Official-Sensitive'
- Accredited to store patient data
- HSCN Peering Exchange Provider
- Accredited to connect and supply over Public Services Network (PSN)
- Accredited and experienced G-Cloud supplier
- 15+ years of N3 experience
- Fully aligned with ITIL Service Management Standards
- ISO 9001, 14001, 27001, 22301 and 20000-1 certified
- Cyber Essentials and Cyber Essentials Plus certified
- PCI Compliant for physical hosting services
- Services designed, built, implemented and supported using appropriate NSCS GPSs, Cabinet Office and NHS Digital standards
- Fully approved HSCN connectivity to Azure and AWS environments.

17. Why choose Redcentric?



Owned infrastructure

We believe that service quality is dependent on end-to-end control and capability, which is why we've spent the past three decades building our own infrastructure and skills base: a UK-wide MPLS network, UK-based data centres, Voice and IaaS platforms, Network and Security Operations Centre, and a large ITIL-based support operation.



Expert guide

We are not about the provision of one-off IT commodities but rather helping clients over the short, medium and long-term through the strategic alignment of our services to organisational requirements. We guide you on your journey at whatever speed and in whatever direction the need dictates.



Customer-centric culture

It is the 'can do' attitude of our teams that we are most proud of and which our customers most value and often comment on. We invest in our staff and work hard to develop and preserve a culture that prioritises staff satisfaction and motivation. We believe that the happier, more engaged, and dynamic we are as a team, the more we can achieve together, ensuring we deliver the best results for our customers.



Open-minded and innovative

We pride ourselves on being an innovative service organisation which means we are always willing to think and do differently and to go beyond norms and conventions. We are always reviewing our proposition, introducing new proven technologies that dovetail with our existing offering; and bringing these opportunities for further gains to our customers. But equally this spirit of innovation may be seen in our flexible approach to project management, and it extends to all aspects of how we work with our customers.



Breadth of services

Our great strength is our ability to be a single unifying partner who can deliver a comprehensive range of IT and Telecoms services across multiple sites with confidence.



Security and integrity

We invest in our systems and processes, that in turn allow us to attain the highest standards of certification and accreditation. These are not badges of honour, but hard-earned evidence of our commitment to quality, security, and integrity, and this supports our aim to be a 'trusted partner'.



Outcomes focused

We believe we have an important role to play in ensuring you have the IT infrastructure and services to help you to achieve your goals. We help you to meet new challenges and to stay agile so that you can respond to change and at the same time keep your data and systems highly secure.



Our teams

We have highly skilled staff, whose average tenure is more than 10 years bringing a huge wealth of experience and a depth of knowledge on which you can rely. We also invest in the development of new team members who bring new or enhanced skills to Redcentric and the training of existing staff to ensure you benefit from a consistent, high-grade delivery of services and support day in, day out.



Continuous Service Improvement

We are committed to investing the most that we can to build a sustainable, successful business that can deliver genuine IT outcomes for our customers. We are continually refreshing our core systems or adding capacity and capability, to the tune of many millions.



Proactive

We think and
act quickly



Inspired

We create
excitement through
innovation

Trusted

We do what
we say we will

Collaborative

We work together
to deliver
a common goal

Transparent

We are open,
honest and fair





Head office

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522

E sayhello@redcentricplc.com

W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED

