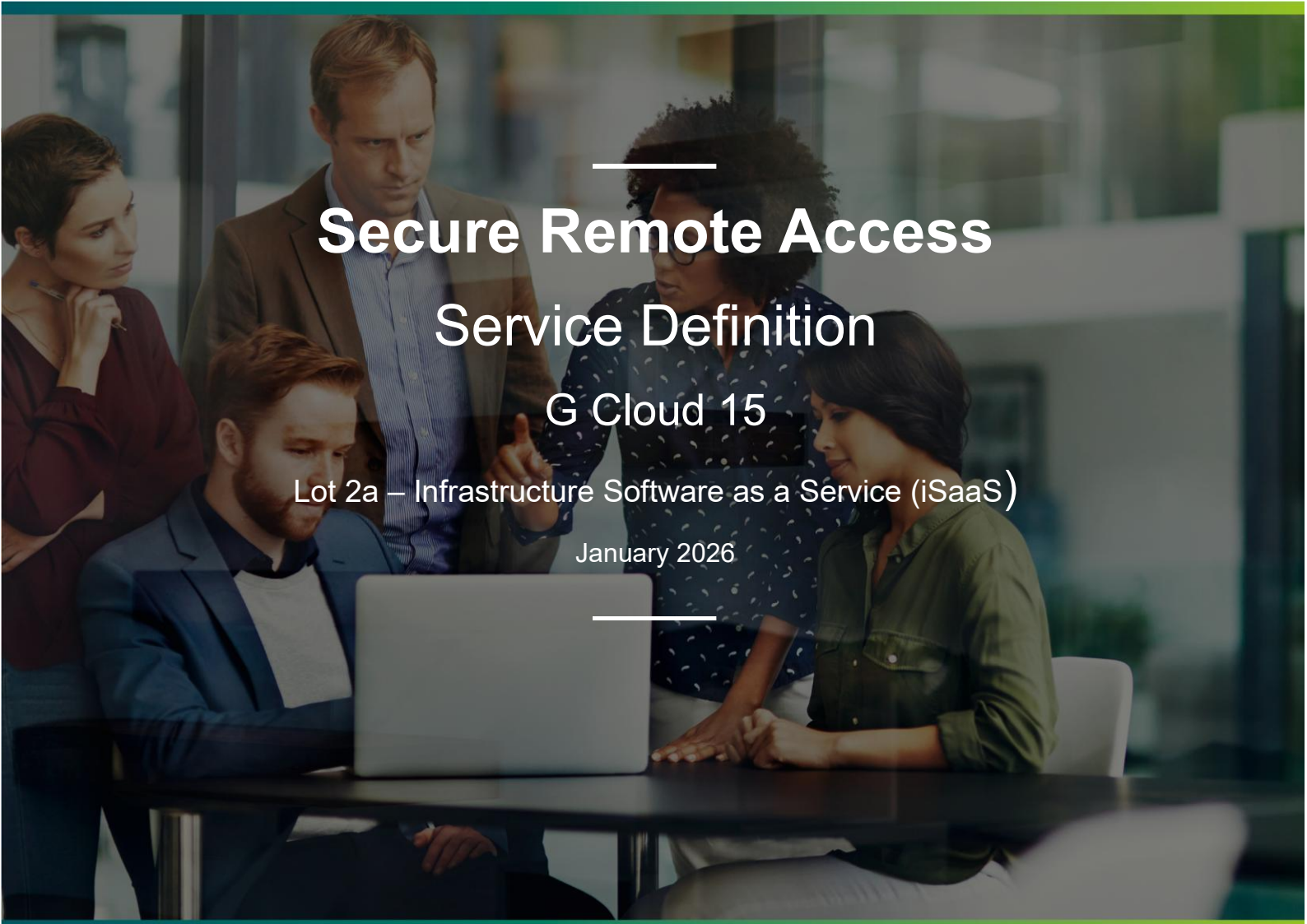




Secure Remote Access

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
1.2 Benefits	4
2. Service Description	5
2.1 Remote access solution	5
2.2 Basic operation	5
2.3 VPN client software	5
2.4 Authentication token types	6
2.5 Mixing, changing, and issuing multiple tokens	6
2.6 Ordering and Service Set-up	6
2.7 Replacement authentication fobs	6
2.8 Administration portal	6
2.9 LDAP agent	7
2.10 Monitoring	7
2.11 Support	7
2.12 Documentation & training	7
2.13 Reporting	7
2.14 Simultaneous use, contention, and fair use policy	7
2.15 Hardware ownership	7
3. Onboarding and Offboarding	8
3.1 Onboarding	8
3.2 Acceptance criteria	8
3.3 Offboarding	8
4. Associated Redcentric Services	9
5. Service Levels and Service Credits	10
5.1 Service Levels	10
5.2 Floor Service Level	10
5.3 Service Credits	10
6. Responsibilities and Accountabilities	11
6.1 High Level Redcentric Responsibilities	11
7. Data Processing	12
7.1 Data processing scope	12
7.2 Data storage and encryption	12
7.3 Data processing decisions	12
7.4 Sub-processors	12
7.5 Customer access to data	12
7.6 Security arrangements and options	12
8. Business Continuity and Disaster Recovery	14
8.1 Business Continuity	14

8.2 Disaster Recovery.....	14
9. Exit Plan.....	15
10. Project management	16
11. Account management	18
12. Service management.....	19
13. Support Services	20
14. Information assurance	21
15. Professional services.....	22
16. Company profile	23
17. Why choose Redcentric?	24

1. Service Overview

1.1 Service overview

Redcentric Secure Remote Access (SRA) Service offers a robust, flexible, and secure way for remote workers to access information and business applications whilst away from their usual work location.

A piece of software on the user's PC, tablet or other remote device communicates with the resilient Redcentric remote access platform across a ubiquitous Internet connection and a secure tunnel is built between the two. The user's data is passed through this tunnel, then from the remote access platform to the corporate network where traffic is routed to its destination. The Secure Remote Access Service includes highly secure two-factor authentication to ensure that only legitimate users can connect. Strong encryption is implemented on the tunnel between the user and the platform to protect sensitive information in transit.

1.2 Benefits

- Facilitates remote working. Enables frontline staff to access key resources remotely
- Supports business continuity. Allows users to continue working away from their formally connected offices, enabling business continuity and recovery from disastrous events
- Increased front-end focus. Allows Customers to concentrate on their core business activities
- Scalable and flexible. Delivers best-of-breed remote access connectivity and can scale easily to meet the needs of Customers large and small
- Access to value-adding service propositions. Designed to support and enhance the entire Redcentric portfolio of services

2. Service Description

2.1 Remote access solution

A small piece of software is deployed on the end-user's laptop (or similar). With suitable Internet access (possibly Wi-Fi or mobile Internet connection), and when initiated by the user, the software builds a secure communication tunnel across the Internet to Redcentric remote access platform. The end user identifies them self to the platform using a supplied software authentication token which can run on a laptop, MAC, or smartphone (or optional hardware fob). This user authentication is dependent on two factors; something the user knows and something the user has. When prompted for authentication, the user inputs a pin-code they have memorised plus the output from the token. This robust, secure authentication, in conjunction with the encryption applied to the data tunnel, meets the stringent security requirements of most modern corporate organisations.

2.2 Basic operation

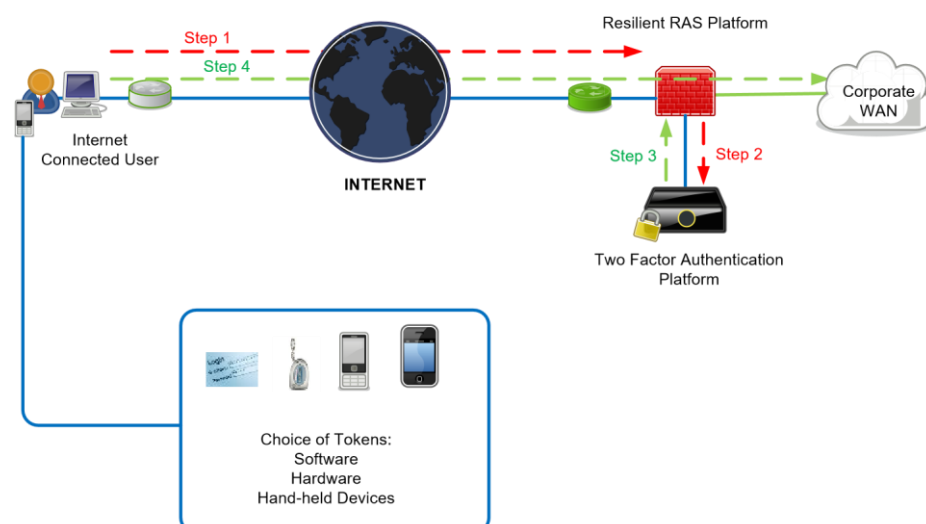
The steps shown in the diagram below illustrate how users are connected to their corporate network from a remote location:

Step 1: The user establishes a connection to the platform using preconfigured client software which is loaded on their end device. During negotiation, the user presents their username and authentication credentials i.e., Factor1 - Their PIN and Factor-2 - The output from their token (also supplied)

Step 2: The remote access platform sends the user's credentials to the two-factor authentication platform

Step 3: The authentication platform validates the user's credentials

Step 4: Assuming the user is authenticated, the encrypted tunnel is built, and the user is provided access to their corporate network and its resources



2.3 VPN client software

Most modern Operating Systems on laptops and other mobile devices include a suitable VPN client. However, Redcentric also supplies a client that can be used on a wide variety of devices and operating systems including Microsoft Windows and Apple Mac OS X.

2.4 Authentication token types

Redcentric offers both software and hardware tokens.

Software tokens can be deployed on tablets, laptops, and smart phones. Software tokens reduce the cost of ownership as they are easier to deploy and can be re-issued to an alternative device as required.

The hardware token option can be used when no laptop, tablet or smart phone is available. Its low weight and size make it ideal for use on a keyring, but consideration needs to be made to battery-life and the greater potential for loss, damage, and increased likelihood of losing synchronisation. Redcentric supports software tokens on the following Operating System platforms:

- Apple iOS
- Android
- Windows phone
- Mac OS
- Windows desktop

2.5 Mixing, changing, and issuing multiple tokens

It is possible to order a combination of software and hardware tokens across a group of users. For example, it is possible to deploy software tokens on laptops of 30% of users, software tokens on smartphones of 60% of users and issue the remaining 10% of users with hardware tokens.

It is not possible to swap between software and hardware tokens during the term of the contract.

A single user can be issued with more than one token, but this has a charging implication as the service charge is based on the number of token licenses on the system, as well as the number of users.

2.6 Ordering and Service Set-up

Under normal circumstances, initial and additional user licences would take no more than 15 working days to commission on the platform.

2.7 Replacement authentication fobs

Redcentric will replace hardware tokens that develop a fault at no charge during the term of the contract.

Customers with a large estate of hardware tokens are advised to order extra units in advance, to replace tokens that become lost or damaged.

Customers are required to order hardware tokens to replace those where the battery reaches the end of its useful life (typically four years or more).

Software tokens cannot be lost, damaged or become faulty; they can be re-issued, as required, via the administration portal.

2.8 Administration portal

As part of the SRA Service, Redcentric provides access to an administration portal. The Customer's help desk staff use the portal to provide support to end users according to the Customer's internal service levels for straight-forward tasks, e.g., soft token re-issue and user password re-sets.

One SRA token/licence is required for each of the Customer's administrators. To enforce security, administrators are required to use the system to log on to the administration portal.

2.9 LDAP agent

Optionally, a Lightweight Directory Access Protocol (LDAP) synchronization agent is available for Customers to deploy in their environment. Once installed, the agent monitors LDAP groups for membership changes and updates user information on the authentication platform to reflect these changes. The agent reads only basic information from the directory and communication from the agent to the authentication platform uses strong encryption. Specific details of the LDAP agent, including the directories that can be supported, is available on request. LDAP agent set-up and support incurs additional charges.

2.10 Monitoring

Redcentric monitors the remote access platform for availability and performance against pre-determined criteria. Redcentric periodically sends an authentication request from a remote device to the authentication platform to ensure that the platform is operating correctly and returning authentication responses. Response time-out, authentication failure of test polls and platform issues automatically trigger the creation of a fault ticket, and the issue is subsequently investigated by a Redcentric engineer.

2.11 Support

Redcentric staff support the platform, the administration portal and provide system wide support to the Customer's help desk staff. Redcentric do not offer support directly to end users.

2.12 Documentation & training

Redcentric will provide a user guide and an administrator's guide. In addition, and if required, Redcentric will provide telephone support as the Customer adds the first few users to the system via the administration portal.

2.13 Reporting

An extensive selection of reports can be accessed from the Authentication Administration Portal including, for example, authentication history, token counts & inactive users. No reporting information is available regarding the amounts of data transferred.

2.14 Simultaneous use, contention, and fair use policy

The platform has been designed to meet the Service Levels set out in section 4 under standard operating conditions. The SRA Service has been built to meet most Customer's needs and to make it cost effective, the platform is built on the basis that only a fraction of potential users will connect at any one time, however various ratios of potential users to allowable connections are available, up to a 1:1 contention ratio, where all a Customer's users are able to connect simultaneously. Increased user contention ratios may incur additional charges. If a customer persistently consumes a disproportionate amount of capacity, to the detriment of other Customers, that Customer may have limits applied to the resource they can consume including a limit on their maximum number of simultaneous connections.

2.15 Hardware ownership

Redcentric remains the owner of hardware tokens until the SRA Service terminates, when ownership of hardware tokens is transferred to the Customer. The Customer is required to dispose of hardware tokens in accordance with Waste Electrical and Electronic Equipment recycling (WEEE) regulations or return them to Redcentric in a single batch for disposal when the 2FA Service terminates.

3. Onboarding and Offboarding

3.1 Onboarding

Our projects and delivery teams work closely with customers to bring services into commissioned state, providing engineering support and guidance as necessary. Engineers setup the service and then hand the service over to the customer.

3.2 Acceptance criteria

The following are the Acceptance Criteria applicable to the Secure Remote Access Service:

- Delivery of hardware tokens to Customer
- User guide supplied to Customer
- Administrator guide supplied to Customer
- Supply of client software to Customer
- One Customer administrator account set-up on the administration portal
- Customer administrator can access portal and confirms licences are in the resource pool
- Token allocation and user set-up for at least one end user – with support from Redcentric if required
- Test to confirm that end user can connect to the platform and ping devices in the Customer's corporate network

3.3 Offboarding

Our projects, delivery and support teams work closely with customers to bring services out of commissioned state, providing engineering support and guidance as necessary. Where required, our support teams work with customers to provide any reporting or log data from the service at the point of decommissioning and to cease billing.

4. Associated Redcentric Services

The table below provides details of other compatible services available from Redcentric via 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 Local Area Network (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 Secure Remote Access service is as follows:

Service Level:	Service Availability:
Service Level	Not less than 99.99%

5.2 Floor Service Level

The Floor Service Level applicable to the Secure Remote Access service in respect of Availability shall be 85% in any given Month.

5.3 Service Credits

The Service Credits applicable to the Secure Remote Access service shall be calculated as follows:

In the following table:

“≥” means “greater than or equal to”

“<” means “less than”

“**MS**” means the total Charges payable in respect of the Secure Remote Access service for the same Month

Service Availability	Service Credit
≥ 99.99%	none
≥ 99.0% but < 99.99%	5% of MS
≥ 97.0% but < 99.0%	15% of MS
< 97.0%	20% of MS

6. Responsibilities and Accountabilities

6.1 High Level Redcentric Responsibilities

As part of the Secure Remote Access service, Redcentric performs the following functions:

- Configures the Customer environment on the remote access and authentication platforms
- Loads token licences onto the platform
- Provides the Customer with VPN client software
- Despatches hardware authentication tokens to a single Customer location usually in a single shipment
- Configures the platform to access the Customer's Redcentric wide area network according to the solution design
- Maintains the resilient, centralised authentication and remote access platforms

6.2 High Level Customer Responsibilities

The Customer is responsible for:

- Distribution, set-up, and support of remote VPN software to individual users and their respective devices
- Identifying and sourcing suitable VPN software for device / operating systems combinations not supported on the supplied software
- Adding user details to the platform, and allocating each user a token licence
- Triggering the software token allocation for each user or physically allocating hardware tokens to users
- Undertaking user support and administration using the administration portal (e.g., user password reset)
- Returning faulty hardware tokens to Redcentric (in batches)
- Making provision for suitable Internet connectivity for end users
- Timely ordering and distribution of replacement hardware tokens when the internal battery reaches end-of-life

7. Data Processing

7.1 Data processing scope

The Secure Remote Access Service facilitates secure transport of IP packets between remote workers and the Customer's corporate network and does not involve any storage or backing up of data.

7.2 Data storage and encryption

Industry standard encryption protocols are used to help keep user traffic traversing the Internet private. Customer data traverses the public Internet between the remote user and the Secure Remote Access Service platform gateway. Redcentric uses multiple upstream tier-1 Internet Service Providers (e.g., Cogent, Lumen and LINX etc.) for Internet connectivity. Redcentric has no control of traffic that traverses the Internet with regards integrity, confidentiality and/or reliability. Consequently, the Secure Remote Access Service platform makes use of user authentication and data encryption to help maintain Customer data confidentiality and integrity.

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 IP packet corruption. Such diagnosis would involve the examination of a small sample of IP packets. This would only be undertaken at the request of and in conjunction with the Customer.

7.3 Data processing decisions

Redcentric does not make any data processing decisions in relation to the Secure Remote Access Service. Any processing of data over Customer systems when using the Secure Remote Access 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 Secure Remote Access 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.

7.4 Sub-processors

Redcentric uses a product from third party company, Thales, to implement multi-factor user authentication. Thales hold basic credentials of remote users only. Otherwise, Thales does not have access to Customer data.

No other third parties are involved in delivering the Secure Remote Access Service, and there are no sub-processors appointed by Redcentric.

7.5 Customer access to data

The Customer controls its own platforms which use the Secure Remote Access Service to carry data for authentication, and the Customer therefore has full access to its own data on those platforms.

7.6 Security arrangements and options

The core Infrastructure delivering the Secure Remote Access Service is hosted at both Redcentric and third-party locations.

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

8. Business Continuity and Disaster Recovery

8.1 Business Continuity

Redcentric complies with Business Continuity ISO 22301:2019 and operates and maintains a robust Business Continuity Management System (BCMS). The BCMS scope includes;

- Data Centres
- 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 Centres, 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 as 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 used are from market leaders 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.

8.2 Disaster Recovery

There is no disaster recovery per se as part of this service, since multiple levels of resiliency are built in, and this service employs geographical resilience by design.

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.

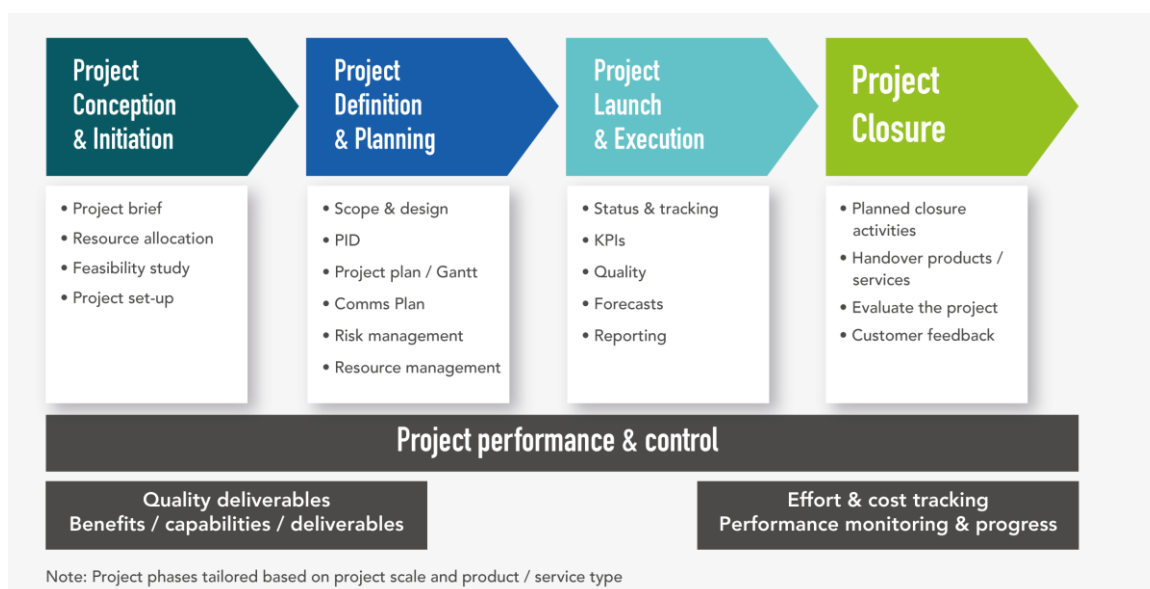
10. Project management

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

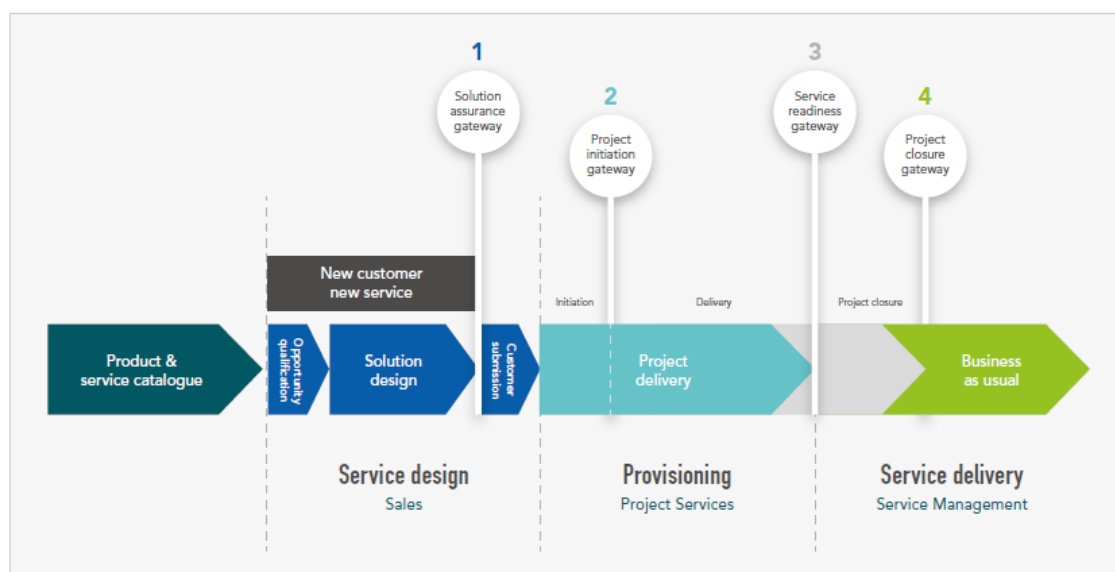
- Test plan to minimise disruption to your business operations
- Communications plan that defines what information to share and with whom
- Site implementation tracker to record the migration progress
- Weekly highlight report providing project updates
- Customer Service Pack
- UAT Test Report – per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

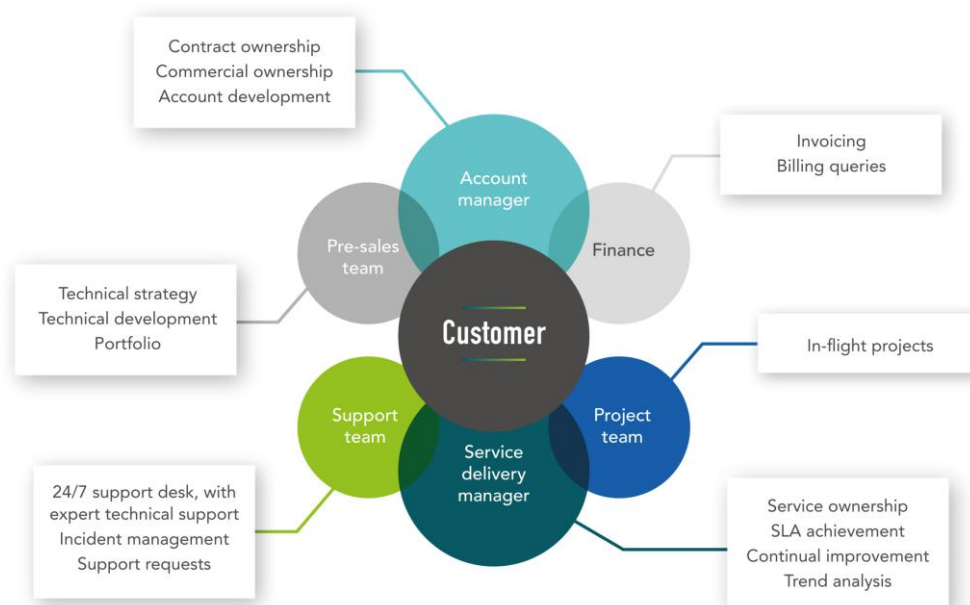
- Technical delivery is achieved on time and to specification
- The support model is fit for purpose and available at service commencement
- You will experience a 'soft landing' with minimal disruption to service.



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

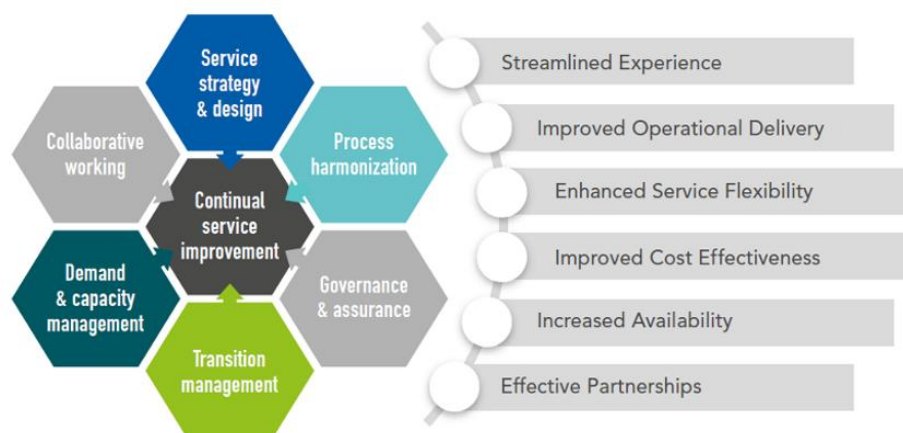
We appreciate the nature of your business demands an exceptional service. We recognise you need to be supported by a team who are not only competent and highly skilled, but also passionate about delivering the right outcome, every time. In our experience, this is achieved by aligning our expertise from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



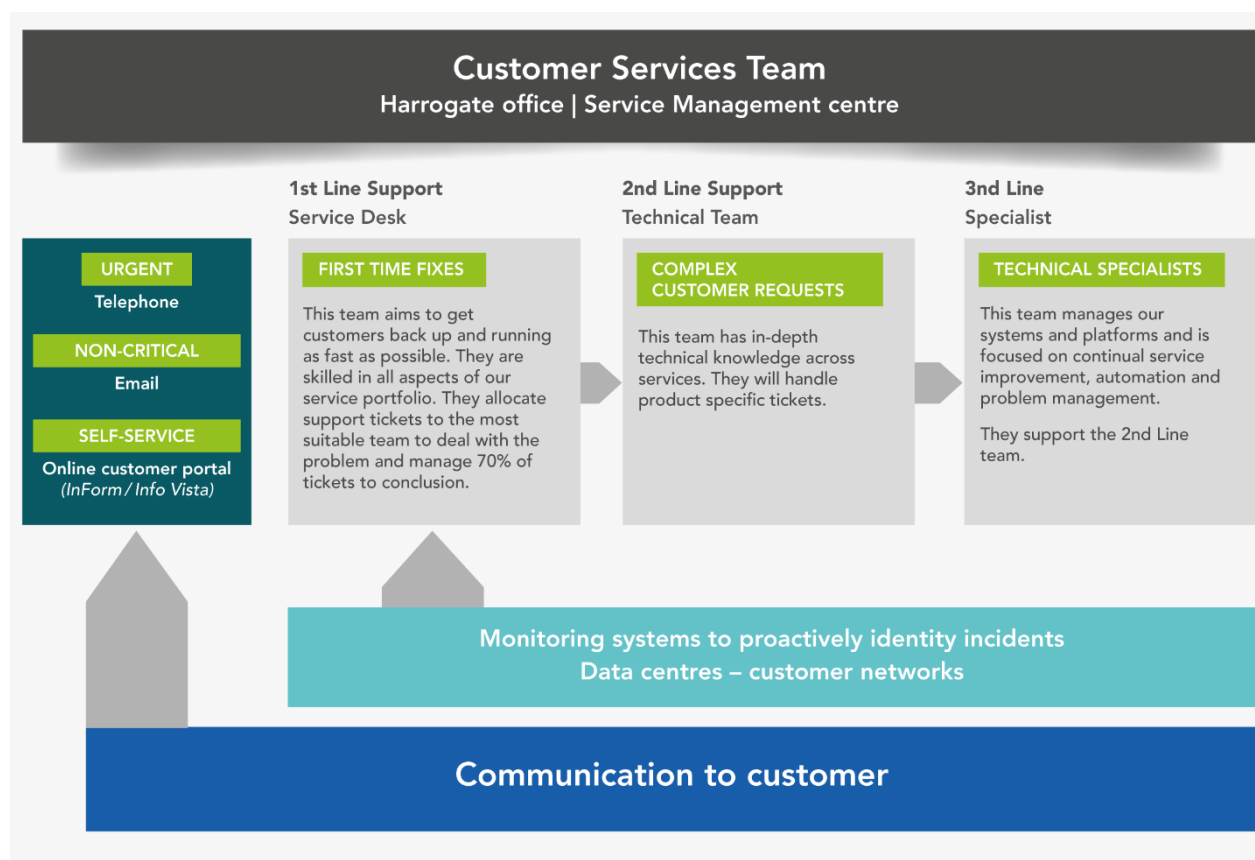
We have thoroughly documented the major incident and customer service plans, which detail how we operate in business-as-usual scenarios and during major incidents.



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

