Managed Vulnerability Scanning

Service Definition

G Cloud 14

Lot 3 – Cloud Support

April 2024

redcentric

AGILE • AVAILABLE • ASSURED

Contents

A message from our CEO

We have been part of G-Cloud since its launch and have long-term relationships with many organisations within the public sector, helping them to gain the benefits of digital transformation. Our commitment and focus remain as clear and strong as ever – to help you to transform, modernise and evolve your IT infrastructures and to be trusted to work closely with your teams to deliver the quality, success, and value you expect.

Our customers tell us that they most value our ability to guide and support them as a strategic partner. We provide value by leveraging knowledge of your marketplace, acquired through long-term relationships with many different public sector organisations. We help you to navigate major changes to infrastructure, working closely alongside your teams, delivering complex projects, across multiple technologies.

We offer one of the most comprehensive ranges of cloud services available in the marketplace through our continued investment in our infrastructure and our strategic partnerships. This means we can deliver cloud services to fulfil a whole range of different needs. Through our recent acquisitions, we have also added significantly to existing skills within our teams and offer deep expertise across our cloud services group as well as our connectivity, communication, and cyber-security teams. It is the deep knowledge, broad experience and 'can do' approach within our teams that makes a huge difference to our customer relationships.

Our track record under G-Cloud and right across the public sector should give you confidence in our credentials.

For many years, we have enjoyed a close partnership with NHS Digital, our NHS customers, and the ecosystem of healthcare solution providers, helping them to take advantage of everything that cloud services have to offer.

When it comes to security, we are one of only two providers of sovereign cloud in the UK, we deliver cloud services to organisations requiring the highest levels of security. We are trusted partner to the Home Office and have driven innovative change projects at both the Department of Justice and the Department of Work and Pensions, while also winning awards for our work with the Ministry of Defence.

As an enabler for digital transformation and innovation, multi-cloud has become increasingly important. To meet the need for greater flexibility and resilience, we have recently invested in a new IaaS platform using cutting edge VMware CF5 and HPE Greenlake technology. This gives us a platform with hyperscale capabilities for modern applications, while delivering the flexibility and scalability to enable you to optimise infrastructure, to mitigate risk and to drive innovation. It's a game-changer in terms of performance and capabilities, with capabilities which are transformative for our public and commercial sector customers.

We recognise that the cloud journey will be different for everyone, which is why we seek to work closely with you to understand what you're trying to achieve. What is constant for us, is that we endeavour to be the same approachable, professional, trusted partner that has characterised our time on G-Cloud. We're a single point of contact, with broad expertise across a complex IT landscape, ready to help you to inform plans to achieve long-term strategic objectives and to help you to respond to change with agility.

I hope that we have given you all the insight you need to understand our capabilities and 'can do' approach, but if there is anything you would like to ask or clarify, then please contact a member of the Redcentric team and we'll be delighted to help.

Kind regards

Peter Brotherton

CEO, Redcentric

1. Service Definition

The Redcentric Managed Vulnerability Scanning enables organisations to identify, prioritise, and remediate software vulnerabilities affecting their digital infrastructure, applications, and services that can be exploited by a cyber attacker to cause harm to their business.

Redcentric will perform regular vulnerability scanning of the customer's internal and external (internet-facing) assets including but not limited to end user devices, servers, and network devices.

The service is designed to provide organisations with greater insight and actionable information than a typical vulnerability scanning solution by enriching the data indicate which vulnerabilities pose the greatest risk in the context of their exploitability and presenting the information in an easy-to-use dashboard interface based on Jira.

The service benefits from human oversight to complement industry-leading tooling, ensuring findings can be tailored and presented in accordance with business context, and that the customer is able to interact with human operators to query and interpret findings, and determine the best possible course of response and remediation.

1.1. Key Features

- Identify, track, and remediate vulnerabilities as they emerge to reduce susceptibility to exploit-based attacks.
- Prioritise patching and mitigation efforts to manage the risk of vulnerability exploitation.
- Assess vulnerabilities with contextual knowledge and remediate based on true risk scores.

1.2 Key Benefits and Outcomes

- Reduce vulnerability noise due to false positives and low-impact issues to streamline remediation efforts.
- Eliminate complexity by centralising vulnerability management across your organisation with a single provider.
- Remove the time-burden from valuable employees who can be focused on value-adding activities.
- Limit patching disruption to avoid downtime whilst ensuring impactful issues are quickly addressed.
- Improve visibility and track remediations throughout the patching lifecycle.

1.3 Scope of Services

The service scope can fall into one of two possible categories:

- External assets only – only including assets that can be reached over-the-internet without internal network access provisioning.
- Internal and external assets – including both internet accessible assets and assets requiring an internal network connection.

1.3.1 Quantity of hosts

The standard service includes up to 750 hosts in the scope. Additional hosts will need to be ordered.

Assets that are deployed using a standard device build can be de-duplicated to control the number of hosts being scanned, decrease scanning and processing time, and avoid incurring additional costs. For example, a sample of end-user devices can be scanned as opposed to the full user estate.

1.3.2 Quantity of scans

The service includes 12x scans per year (typically 1x per month). Additional full scans more than the 12x annual scans can be performed but will incur a charge. One extra full scan can be performed without incurring an additional charge. Any additional scans will be charged as set out in the Managed Vulnerability Scanning Price Card.

Ad-hoc scans may be performed where there is a requirement to assess smaller subset of assets for vulnerabilities. This should comprise <10% of the total hosts covered by the service.

- The customer shall endeavour to provide reasonable notice of a request to scan of at least five working days.
- If more than 3 ad-hoc scans are required over a rolling 3-month period, then any additional scans may be chargeable.

1.3.3 Scanning environments without external network connectivity

If scanning of environments that do not have internet access is in scope, additional effort will be required to manually update and prepare the scanning agent running on the dedicated server. These charges will be scaled directly to the additional manual effort required and will be provided on a case-by-case basis.

1.3.4 Scanning multiple environments requiring additional scanner hosts

Charges may apply where additional scans are required if not all ranges are reachable from a single host, depending upon the number of additional hosts required.

1.4 Deployment and on-boarding

The customer will provide Redcentric with an asset list encompassing domain and host addresses.

If internal assets are in-scope that are not reachable over the internet, internal servers should be assigned to Redcentric for the deployment of the scanning service. Redcentric uses a network-based (as opposed to agent-based) solution that scans all hosts that are reachable from the allocated server(s) with the scanning software deployed. The server must be a Windows or Linux host that meets the minimum specifications. Redcentric must also be assigned remote access (e.g. via Customer Name’s VPN) and be assigned admin rights to the server.

1.4.1 Server Requirements for internal scanning

The minimum requirements for any internal scanner hosts can be found here: https://docs.tenable.com/general-requirements/Content/NessusScannerHardwareRequirements.htm

1.5 Sub-contractors

There shall be no subcontractors associated with this service.

2. Service Options

2.1. Customer Obligations

- The customer will be responsible for updating the details of network ranges if there are any changes to the scope during the period of the contract.
- The customer will be responsible for the setup and maintenance of the internal server used to deliver the scanning platform.
- The customer will be responsible for the creation of service accounts as required.
- The customer will be responsible for network configuration allowing remote access from the Redcentric remote locations to the vulnerability scanning devices.
- The customer will be responsible for network configuration allowing access from the vulnerability scanning devices to all in scope systems.
- The customer will gain the appropriate approval from any third-party hosting / support services as required.
- The customer will be provisioned with a maximum of six accounts within the Clarus portal. Each account to be assigned to a named individual within the customer's organisation.

2.2. Supplier Obligations

- Redcentric will be responsible for the configuration of the scanning platform to deliver the required ongoing vulnerability scanning service.
- Redcentric will respond to queries made via the Clarus platform within a maximum 7 days of a communication being logged (typical response times are within 48 hours).
- Redcentric will be responsible for analysing the output from the scanning platform.
- Redcentric will be responsible for the creation and maintenance of the Clarus Portal.
- Redcentric will not be responsible for the remediation of vulnerabilities.
- Core service delivery will be limited to twelve monthly scans per year (1x per month). This does not include the ad-hoc scans specified.

3. Service Options

3.1 Regular scanning

Vulnerability scanning of all assets within scope will be scheduled via the vulnerability scanning platform, in-line with the agreed scanning periodicity. Our cloud-based scanning platform will be utilised to scan externally facing assets.

Clarus utilises the Nessus vulnerability scanning engine. Nessus is an industry leading solution that maintains more than 78,000+ vulnerability identification signatures, covering both local and remote security flaws. Nessus can be configured to deliver credentialed and uncredentialed checks against multiple technology platforms.

3.2 Data Enrichment

The data set is exported from Nessus and cross-referenced with the Redcentric vulnerability scoring database and relevant external sources such as the Known Exploited Vulnerabilities (KEV) database and the Exploit Prediction Scoring System (EPSS). This provides additional metrics that can be used to calculate the risk score of the issue and guide remediation priority and urgency.

To enhance our risk assessment, we consider, for example:

- Whether exploit code exists on the public internet.
- Whether exploit code is likely to become publicly available in the future.
- The extent to which the vulnerability has been exploited previously.
- How we have classified the issue previously as part of penetration testing and incident response.
- How the customer has internally risk assessed the type of vulnerability previously.

3.3 Assessment

We will utilise a differential approach to the output, looking to identify changes from the initial benchmark. These will be classified as follows:

- New vulnerability introduced to the environment - Where a new vulnerability is identified, we will review the technical output to confirm the validity of the issue (removing common false-positives) and pass to the triage and escalation stage.
- Removal of vulnerability from the environment - Where a previously identified vulnerability has been remediated and confirmed through ongoing vulnerability scanning, the remediation tracker will be updated to reflect the change in status of the issue.
- Change in severity - Changes within the threat landscape can have an impact on the relative severity rating of known vulnerabilities. Where this occurs, we will review all severity ratings associated with that change and apply new severity ratings as required.

3.4 Triage and Escalation

Where a new vulnerability is identified, we will review the technical output and assign a priority level and update the remediation tracker. Where a vulnerability is categorised as critical, we will report as agreed within the escalation plan. Otherwise, new vulnerabilities will be managed as part of the ongoing remediation tracking workflow.

3.5 Remediation Tracking

After the triage and escalation phase, all technical details relating to individual vulnerabilities will be uploaded to the Clarus portal for access by the customer. The remediation tracker utilises a ticketing-based system to track individual vulnerable hosts along with the overarching vulnerability exposure. The tracker focuses on four swim lanes, ‘Backlog’ - contains details of new vulnerabilities found, ‘In Progress’ - captures tickets that have been allocated for remediation activity, ‘Risk Accepted’ - captures any vulnerability where the customer has chosen to accept the risk and finally, ‘Remediated’, for issues where the customer has completed remediation activity to close the item.

3.6 Remediation Validation

During each subsequent vulnerability scan hosts will be checked against existing vulnerabilities, if all hosts within a defined vulnerability category are identified as no longer being vulnerable, the ticket is automatically moved to the ‘Remediated’ column.

3.7 Reporting

Ongoing scanning will be delivered monthly for both internal and external network assets. The output will be triaged and processed by the Redcentric team and then uploaded to the Clarus portal, where the findings will be presented to the customer team for remediation.

After the completion of each monthly scan a reporting email will be generated providing a summary of the findings and any key changes from the previous scan.

Redcentric will make its consultants available for a debrief session each month that can be used as an opportunity for the customer to ask questions about the findings and establish a remediation plan under the guidance of Redcentric consultants.

The customer will be provisioned with a maximum of six accounts within the Clarus portal. Each account is to be assigned to a named individual within the customer’s organisation. Additional reporting capability exists within the platform for wider distribution of relevant information to individual support teams for the purposes of remediation.

4. Associated Redcentric Services

The tables below provide details of other Redcentric services available from G-Cloud 14.

4.1 Lot 1 Cloud Hosting

Service Name	Service Summary
Access as a Service	**Access 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. This service is compatible with **DDoS Mitigation Service, Managed Firewall Service. Managed LAN Switch Service, Meraki Connectivity and Security Service, Managed SD-WAN Service. Managed Wireless LAN Service, Wireless Guest Access Service**
Backup as a Service	**Backup as a Service (BaaS)** is a cloud based, data protection, and disaster recovery solution that supports a wide array of applications, data types, and workloads, including endpoints. It also provides vulnerability scanning, patch management, remote desktop, and health reports, along with next generation AI-based protection against malware via an easy-to-use customer portal and interfaces. This service is compatible with **Cyber Security Services, Disaster Recovery as a Service, Infrastructure Recovery, Physical Workplace, Redcentric Cloud, Storage as a Service**
Database as a Service	**Database as a Service** is an ITIL aligned standard, repeatable database infrastructure, provisioning, and administration service for SQL Server database management systems. Priced on a per instance basis for the service element and consumption and licensing costs for infrastructure and provisioning. The product is delivered remotely using standard processes, tools, and automation. The service is compatible with **Disaster Recovery as a Service, Storage as a Service, Managed Public Cloud AWS, Managed Public Cloud Azure, Monitoring as a Service, Managed Server as a Service, Redcentric Cloud, Redcentric Sovereign Cloud**
DDOS Mitigation Service	**DDoS Mitigation Service** consists of three services. DDoS Essentials and DDoS Essentials Plus, ensures customer protection within 60 or 15 minutes respectively, upon attack notification. DDoS Pro offers comprehensive management with instant detection and automated response. Monitoring at the ISP level enables pro-active attack identification, enhancing network security measures. The service is compatible with **Access as a Service. Managed Firewall Service, Meraki Connectivity and Security Service. Managed SD-WAN Service**
Disaster Recovery as a Service	**Disaster Recovery as a Service** managed service ensures that your production environment is protected, and it provides continuity in the event of a disaster. It enables you to speedily recover your business-critical applications & data and resume essential business activities within hours, rather than days. The service is compatible with **Access as a Service, Backup as a Service, Cyber Security Professional Services, Infrastructure Recovery, Physical Workplace, Storage as a Service.**
Healthcare Secure Remote Access	**Healthcare Secure Remote Access** service offers a robust, scalable, flexible, and secure way for healthcare professionals to access the HSCN network 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. This is a standalone service.
Infrastructure Recovery	**Infrastructure Recovery** service ensures that in the event of a disaster, you can recover your production environment using Redcentric equipment at our data centres. The service provides customers with a customised environment within our secure data centres based on their specific requirements. The service is compatible with **Access as a Service**, **Backup as a Service, Cyber Security Professional Services, Disaster Recovery as a Service, Physical Workplace**.
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 firewalls control traffic between devices on different networks and provide perimeter

Service Name	Service Summary
	protection. The firewall is configured by our staff to meet customer's requirements. Firewalls are monitored for alerts. The service is compatible with **Access as a Service, DDoS Mitigation Service, Meraki Connectivity and Security Service, Managed SD-WAN Service, Two Factor Authentication Service.**
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. The service is compatible with **Access as a Service, Meraki Connectivity and Security Service, Managed SD-WAN Service, Managed Wireless LAN Service, Wireless Guest Access Service.**
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. The service is compatible **with Access as a Service, DDoS Mitigation Service, Managed Firewall Service, Managed LAN Switch Service, Meraki Connectivity and Security Service, Managed Wireless LAN Service, Secure Remote Access Service, Two Factor Authentication Service, Wireless Guest Access Service**
Managed Server as a Service	**Managed Server as a Service** will manage servers provided on the Redcentric Cloud, hosted physical server services, or managed public cloud infrastructure Managed Public Cloud AWS and Managed Public Cloud Azure. The service provides access to our support capability, technical skills, and economies of scale, to manage the customer's server operating systems. The service is compatible with **Redcentric Cloud, Managed Public Cloud AWS, Managed Public Cloud Azure.**
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. The service is compatible with **Access as a Service, DDoS Mitigation Service, Managed Firewall Service, Managed LAN Switch Service, Meraki Connectivity and Security Service, Managed SD-WAN Service, Wireless Guest Access Service.**
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. The service is compatible with **Access as a Service, DDoS Mitigation Service, Managed Firewall Service, Managed LAN Switch Service, Managed SD-WAN Service, Managed Wireless LAN Service, Secure Remote Access Service, Wireless Guest Access Service.**
Monitoring as a Service	**Monitoring as a Service** is a cloud-based monitoring for cloud and on-premises infrastructure encompassing overall health, performance, and availability of systems, resources, and applications. The customer is provided with standard dashboards and the capability to configure alerts. The customer has near real time information using LogicMonitor cloud-based software delivering modern, informative, and concise metrics. The service is compatible with **Disaster Recovery as a Service, Database as a Service, Storage as a Service, Managed Public Cloud AWS, Managed Public Cloud Azure, Managed Server as a Service, Redcentric Cloud, Redcentric Sovereign Cloud**
Physical Workplace	**Physical Workplace** recovery provides customers with alternative office space and an environment configured for their business. In the event of a disaster staff can move to office space within Redcentric secure recovery centres and continue to work.

Service Name	Service Summary
	The service is compatible with **Access as a Service, Backup as a Service**, **Cyber Security Professional Services, Disaster Recovery as a Service, Infrastructure as a Service.**
Redcentric Cloud	**Redcentric Cloud** is a cloud solution designed to provide a versatile and cost-effective option for Public Sector customers. Delivering virtualised server, storage and network infrastructure using an opex-based consumption model. The platforms are managed by Redcentric covering performance, capacity, patching, installation, upgrades for data marked "official" The service is compatible with **Managed Server as a Service**
Redcentric Sovereign Cloud	**Redcentric Sovereign Cloud** is a community cloud solution for consumption by UK Public Sector organisations, delivering virtualised server, storage and network infrastructure through discreet public sector networks using an opex- based consumption model. The platforms are managed by Redcentric covering performance, capacity, patching, installation, upgrades for data marked "official-sensitive" The service is compatible with **Managed Server as a Service**
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. The service is compatible with **Access as a Service, Managed Firewall Service, Managed LAN Switch Service, Meraki Connectivity and Security Service, Managed SD-WAN Service, Managed Wireless LAN Service.**
Storage as a Service	**Storage as a Service** is an ITIL aligned storage infrastructure, provisioning, and administration service. It provides cost effective resilient storage capacity backed by industry leading vendors (NetApp, Dell) hosted in UK datacentres. The price is per GB basis which includes storage management, infrastructure, licencing, and networking. The service is compatible with **Disaster Recovery as a Service, Database as a Service, Managed Public Cloud AWS, Managed Public Cloud Azure, Monitoring as a Service, Managed Server as a Service, Redcentric Cloud, Redcentric Sovereign Cloud**
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 managed and Redcentric managed network devices. The 2FA service offers a more secure and scalable alternative to static passwords. The service is compatible with **Managed Firewall Service**.
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. The service is compatible with **Managed LAN Switch Service, Managed Wireless LAN Service.**

4.2 Lot 2 Cloud Software

Service Name	Service Summary
Call Recording	**Call Recording** service enables the capture and analysis of conversations, unlocking their full value. The service is compatible with **Microsoft Teams Calling, Unity IP Voice** and **Unity on a SIM.**
Cirrus Omnichannel contact centre	**Cirrus Omnichannel Contact Centre** service elevates public engagement with its: AI-enhanced, omnichannel solutions seamlessly integrated with Microsoft Teams. Experience unparalleled communications across voice and digital channels with advanced AI automation, smart routing, and analytics. Effortlessly scalable, our CCaaS (Contact Centre as a Service) platform ensures top-tier service with end-to-end encryption and data sovereignty.

Service Name	Service Summary
	The service is compatible with **Microsoft Teams Calling, Unity IP Voice** and **Unity on a SIM.**
Microsoft Teams Calling	**Microsoft Teams Calling** from Redcentric provides access to a cost-effective calling capability that enables users to make and receive calls on any Microsoft Teams enabled client or device. The service is compatible with **Call Recording** and **Teams Insights**
Omnichannel Contact Centre for Microsoft Teams	**Omnichannel Contact Centre**, native to Microsoft Teams, gives customers the ability to communicate across several different channels, switching from one to another with ease. Organisations can provide a seamless customer experience by managing those channels effectively to deliver better customer service, improve customer satisfaction and retain loyal customers. The service is compatible with **Call Recording** and **Teams Insights**
Teams Insights	**Teams Insights** offers a comprehensive suite of reporting and analytics tailored for your Microsoft Teams environment. It delivers vital business information through user-defined reports, daily dashboards, and trend monitors, all designed to provide actionable customer insights in an easy-to-understand format. Teams Insights provides accurate, relevant information from which customers can make informed business decisions and effectively manage their organisation's operations. The service is compatible with **Microsoft Teams Calling.**
Unity IP Voice	**Unity IP Voice** is a hosted enterprise voice solution (VoIP) for organisations needing to update their existing telephony system but who are also looking to control equipment, training, and operational costs, and boost the resilience of critical telephony services. The service is compatible with **Call Recording** and **Unity Reporting.**
Unity Reporting	**Unity Reporting** is a secure web-based reporting service that is fully integrated with Redcentric Unity IP voice service. Providing customers with meaningful insights into their ongoing business operations. A feature rich, fully customisable selection of real-time dashboards and historic reports, which are ideally suited to all customer environments. The service is compatible with **Call Recording, Unity Reporting, Unity on a SIM,** and **Cirrus Omnichannel contact centre.**
Unity on a SIM	**Unity on a SIM** service empowers customers to effortlessly transform any unlocked mobile handset into a robust business communication tool. With a comprehensive array of features including DDI numbers, short-dial extensions, call transfer, hunt groups, IVR, voicemail, shared call appearance, and more, it delivers all the essential functionalities expected from a premium business telephony service. The service is compatible with **Unity IP Voice** and **Cirrus Omnichannel contact centre.**

4.3 Lot 3 Cloud Support

Service Name	Service Summary
Cyber Security Professional Services	**Cyber Security Professional Services** Redcentric offers a wide range of Cyber Security Professional Services from strategy to implementation. Aligned to the NIST Cyber Security Framework, our qualified industry professionals will support you in overcoming your cyber security challenges around governance, InfoSec compliance, security testing, vulnerability management, business continuity, disaster recovery, data breach and Incident Response. The service is compatible with **Vulnerability Management Service**
Managed Public Cloud AWS	**Managed Public Cloud AWS**, Redcentric, a next-generation cloud services provider, offers end-to-end lifecycle management. From AWS to Modern Workplace and Azure. We optimise cloud investments. Our expert engineers across multi-disciplines; SRE, SysOps, DevOps, NetOps, FinOps, SecOps and platforms, design multi-cloud strategy; 24/7/365 access to cloud expertise to reduce AWS infrastructure management burdens. The service is compatible with **Modern Workplace 365, Disaster Recovery as a Service, Database as a Service, Storage as a Service, Managed Public Cloud Azure, Managed Server as a Service, Redcentric Cloud, Redcentric Sovereign Cloud**

Service Name	Service Summary
Managed Public Cloud Azure	**Managed Public Cloud Azure,** Redcentric, a next-generation cloud services provider, offers end-to-end lifecycle management. From Modern Workplace to Azure and beyond. We optimise cloud investments. Our expert engineers across multi-disciplines; SRE, SysOps, DevOps, NetOps, FinOps, SecOps and platforms, design multi-cloud strategy; 24/7/365 access to cloud expertise to reduce Azure infrastructure management burdens. The service is compatible with **Modern Workplace 365, Disaster Recovery as a Service, Database as a Service, Storage as a Service, Managed Public Cloud AWS, Managed Server as a Service, Redcentric Cloud, Redcentric Sovereign Cloud**
Modern Workplace 365	**Modern Workplace 365** services represents the future of work, where complexity and risk are minimised, and productivity and collaboration are maximised. This service extends beyond the traditional Managed 365 offering, encompassing a comprehensive modernisation service with digital workspaces and dedicated end-user support. The service is compatible with **Managed Azure, Disaster Recovery as a Service, Database as a Service, Storage as a Service, Managed Public Cloud AWS, Managed Server as a Service, Redcentric Cloud, Redcentric Sovereign Cloud**
Vulnerability Management Service	**Vulnerability Management Service** enables organisations to identify, prioritise, and remediate software vulnerabilities affecting their digital infrastructure, applications, and services that can be exploited by a cyber attacker to cause harm to their business. We will perform regular vulnerability scanning of your internal and external (internet-facing) assets. The service is compatible with **Cyber Security Professional Services**

5. Service Availability

No Service Levels apply with this Service.

6. Responsibilities and Accountabilities

6.1 Customer Obligations

- The customer will be responsible for updating the details of network ranges if there are any changes to the scope during the period of the contract.
- The customer will be responsible for the setup and maintenance of the internal server used to deliver the scanning platform.
- The customer will be responsible for the creation of service accounts as required.
- The customer will be responsible for network configuration allowing remote access from the Redcentric remote locations to the vulnerability scanning devices.
- The customer will be responsible for network configuration allowing access from the vulnerability scanning devices to all in scope systems.
- The customer will gain the appropriate approval from any third-party hosting / support services as required.
- The customer will be provisioned with a maximum of six accounts within the Clarus portal. Each account to be assigned to a named individual within the customer's organisation.

6.2 Supplier Obligations

- Redcentric will be responsible for the configuration of the scanning platform to deliver the required ongoing vulnerability scanning service.
- Redcentric will respond to queries made via the Clarus platform within a maximum 7 days of a communication being logged (typical response times are within 48 hours).
- Redcentric will be responsible for analysing the output from the scanning platform.
- Redcentric will be responsible for the creation and maintenance of the Clarus Portal.
- Redcentric will not be responsible for the remediation of vulnerabilities.
- Core service delivery will be limited to twelve monthly scans per year (1x per month). This does not include the ad-hoc scans specified.

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 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 the core connectivity and routing, and switching devices are used 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.

7.2 Disaster Recovery

No disaster recovery plan is provided as part of these Services.

8. Data

8.1 Data Processing

Note that in completion of this Statement, the CCS Customer is the Controller and Redcentric is the Processor unless otherwise stated. The EU has approved adequacy decision for the UK until 27 June 2025. This Statement is compliant with UK GDPR and the DPA (2018).

8.2 Subject matter of the processing

Redcentric delivers a wide range of cyber security professional services from strategy to implementation. Aligned to the NIST Cyber Security Framework, our qualified industry professionals will support you in overcoming your cyber security challenges around governance, InfoSec compliance, security testing, vulnerability management, BC, DR, data breach and Incident Response.

8.3 Nature and purposes of the processing

All personal data is stored in UK Data Centres unless otherwise stated. Some personal data may be accessed by our Support operation in Hyderabad, India. This access is to authenticate CCS Customer users following a support request or to troubleshoot incidents and is required to satisfy obligations under the Contract. This is subject to controlled remote access using Redcentric owned devices only and is operated under an International Data Transfer Agreement between Redcentric Solutions Limited and Redcentric India.

8.4 Duration of the processing

From the start date of the contract until seven years after the expiry or termination date. It may be necessary to retain data beyond this time according to UK Law.

8.5 Categories of Data Subject International Transfers

It may be necessary for our Support operation in Hyderabad to access personal data to authenticate CCS Customer users following a support request or to troubleshoot incidents. The personal data may include first name, last name, role title, telephone number, which may be checked against a pre-approved list.

8.6 Sub Processors engaged by Redcentric (sub-contractors)

All Redcentric suppliers (sub-processors) are checked for compliance with UK GDPR as part of onboarding and regularly reviewed.

8.7 Types of Personal Data Processed

During Cyber Security Professional Services work the following elements of Personal Data may be processed: first name, last name, telephone number, role title, DDI number, work email address, IP address. The Personal Data to be processed do not include sensitive personal data, or any data the processing of which is restricted (e.g. data relating to criminal offences or convictions)

8.8 Special Category Data

The Personal Data to be processed do not include racial or ethnic origin, genetic data, biometric data, health data, political views, religious beliefs, or trade union membership.

8.9 Data Processing Location

Redcentric Cyber Security Professional Services staff are all UK based, and all personal data is stored in UK Data Centres unless otherwise stated.

9. Exit Plan

At the end of the Contract Redcentric will revoke the client's access to the Clarus portal.

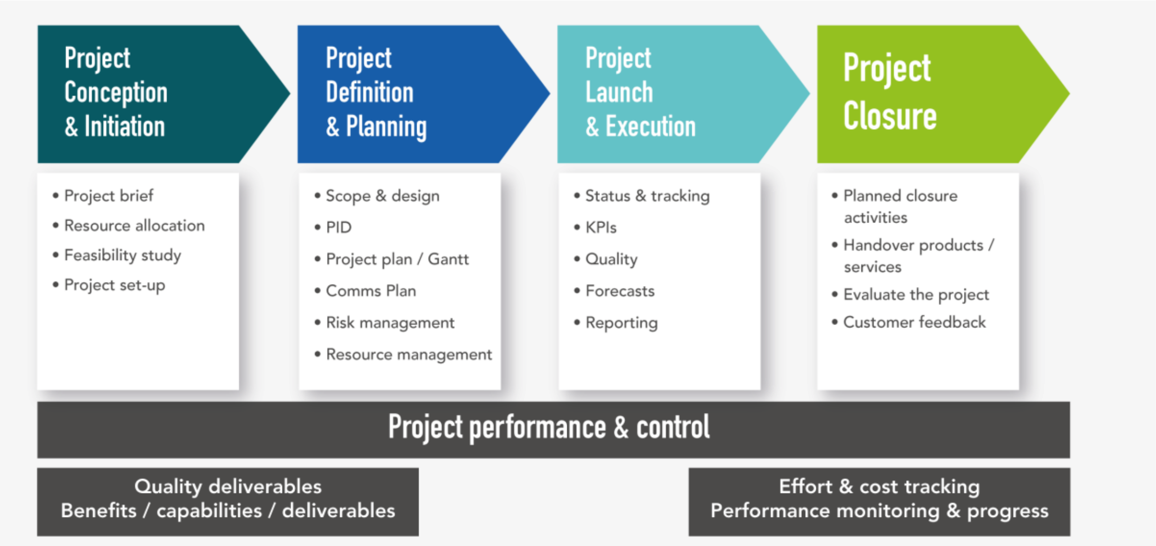
10. Project management

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**



Note: Project phases tailored based on project scale and product / service type

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

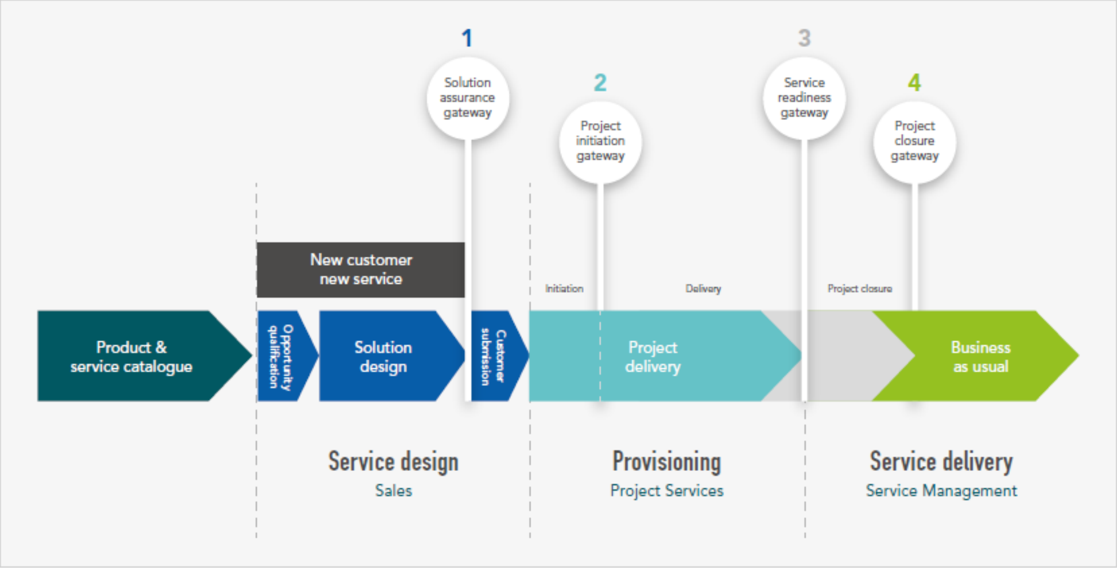
- Test plan to minimise disruption to your business operations
- Communications plan that defines what information to share and with whom
- Site implementation tracker to record the migration progress
- Weekly highlight report providing project updates
- Customer Service Pack
- UAT Test Report – per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

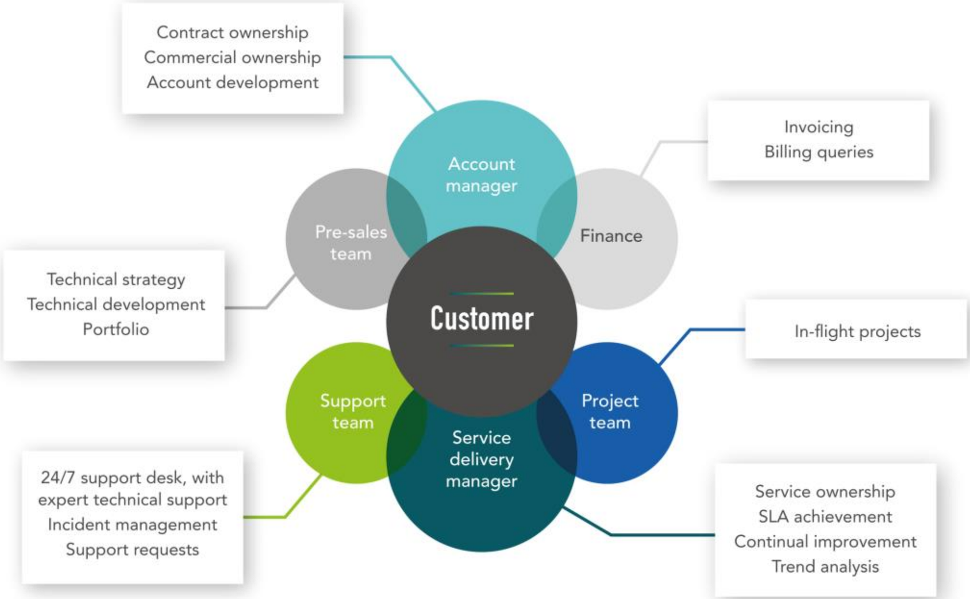
- Technical delivery is achieved on time and to specification
- The support model is fit for purpose and available at service commencement
- You will experience a ‘soft landing’ with minimal disruption to service.



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

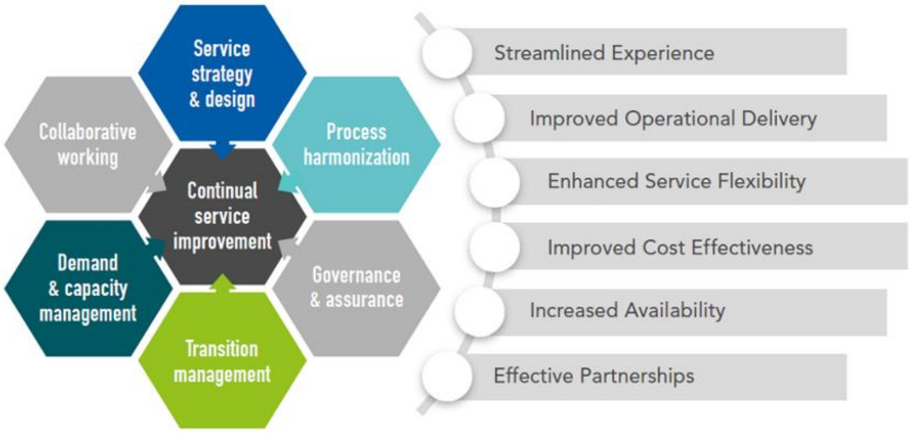
We appreciate the nature of your business demands an exceptional service. We recognise you need to be supported by a team who are not only competent and highly skilled, but also passionate about delivering the right outcome, every time. In our experience, this is achieved by aligning our expertise from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


Service strategy & design
Collaborative working
Process harmonization
Continual service improvement
Demand & capacity management
Governance & assurance
Transition management
Streamlined Experience
Improved Operational Delivery
Enhanced Service Flexibility
Improved Cost Effectiveness
Increased Availability
Effective Partnerships

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.

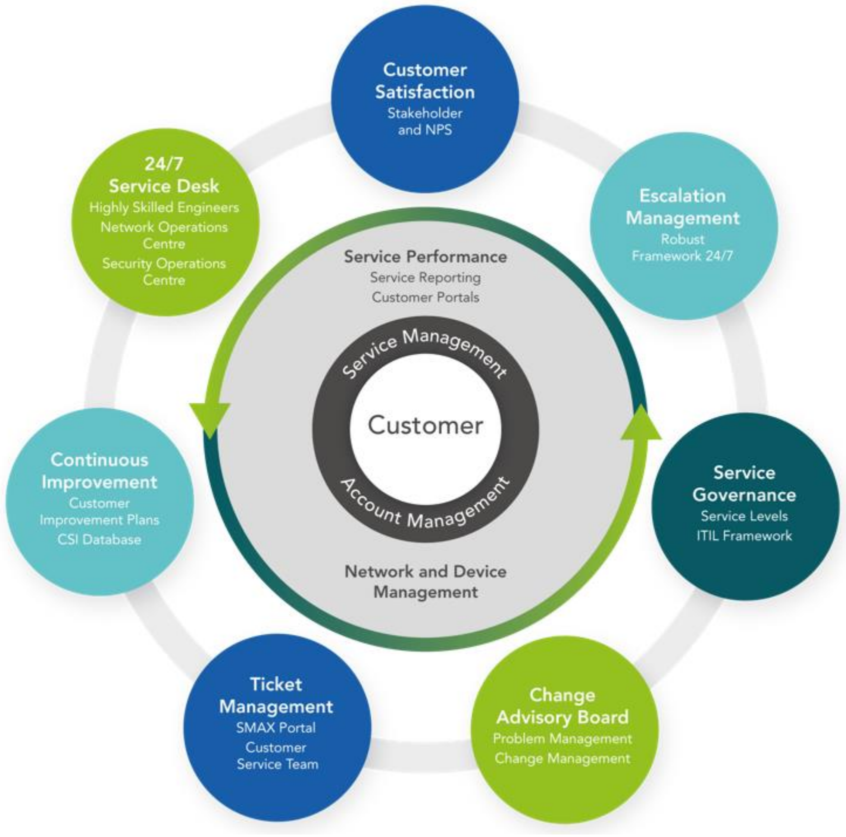
12. Service management

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 2000, which means we have a tried and trusted model for service delivery that provides a consistent approach.

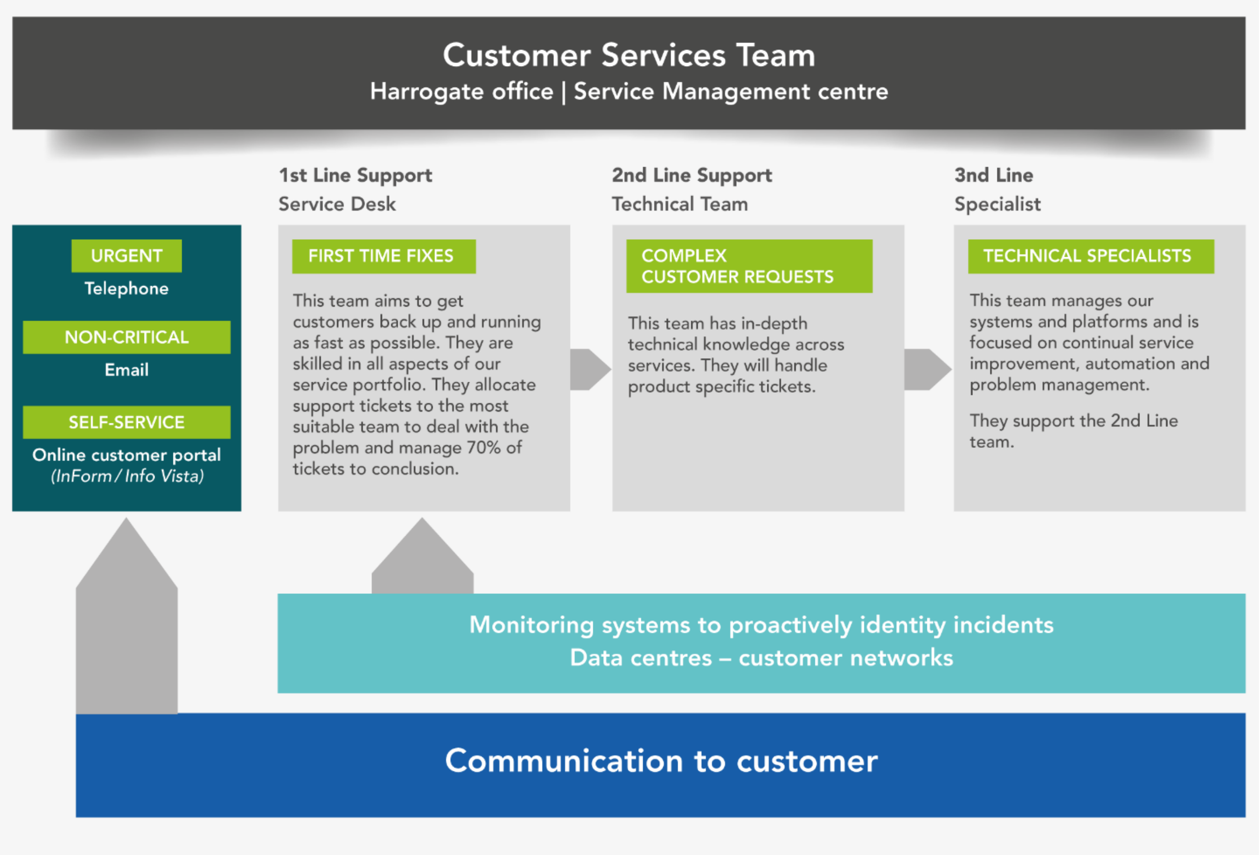
13. Support Services

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.



Customer Services Team
Harrogate office | Service Management centre

URGENT
Telephone

NON-CRITICAL
Email

SELF-SERVICE
Online customer portal
(InForm / Info Vista)

1st Line Support
Service Desk

FIRST TIME FIXES

This team aims to get customers back up and running as fast as possible. They are skilled in all aspects of our service portfolio. They allocate support tickets to the most suitable team to deal with the problem and manage 70% of tickets to conclusion.

2nd Line Support
Technical Team

COMPLEX CUSTOMER REQUESTS

This team has in-depth technical knowledge across services. They will handle product specific tickets.

3nd Line
Specialist

TECHNICAL SPECIALISTS

This team manages our systems and platforms and is focused on continual service improvement, automation and problem management.

They support the 2nd Line team.

Monitoring systems to proactively identity incidents
Data centres – customer networks

Communication to customer

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 27001:2013 Information Security Certified
- 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 and are defined and priced upon application.

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

- 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.

owned UK data centres

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

bsi.

ISO 9001 Quality Management	ISO 14001 Environmental Management	ISO/IEC 20000-1 Information Technology Service Management	ISO 22301 Business Continuity Management	ISO/IEC 27001 Information Security Management
FS 603185	EMS 673082	ITMS 668453	BCMS 603184	IS 603187