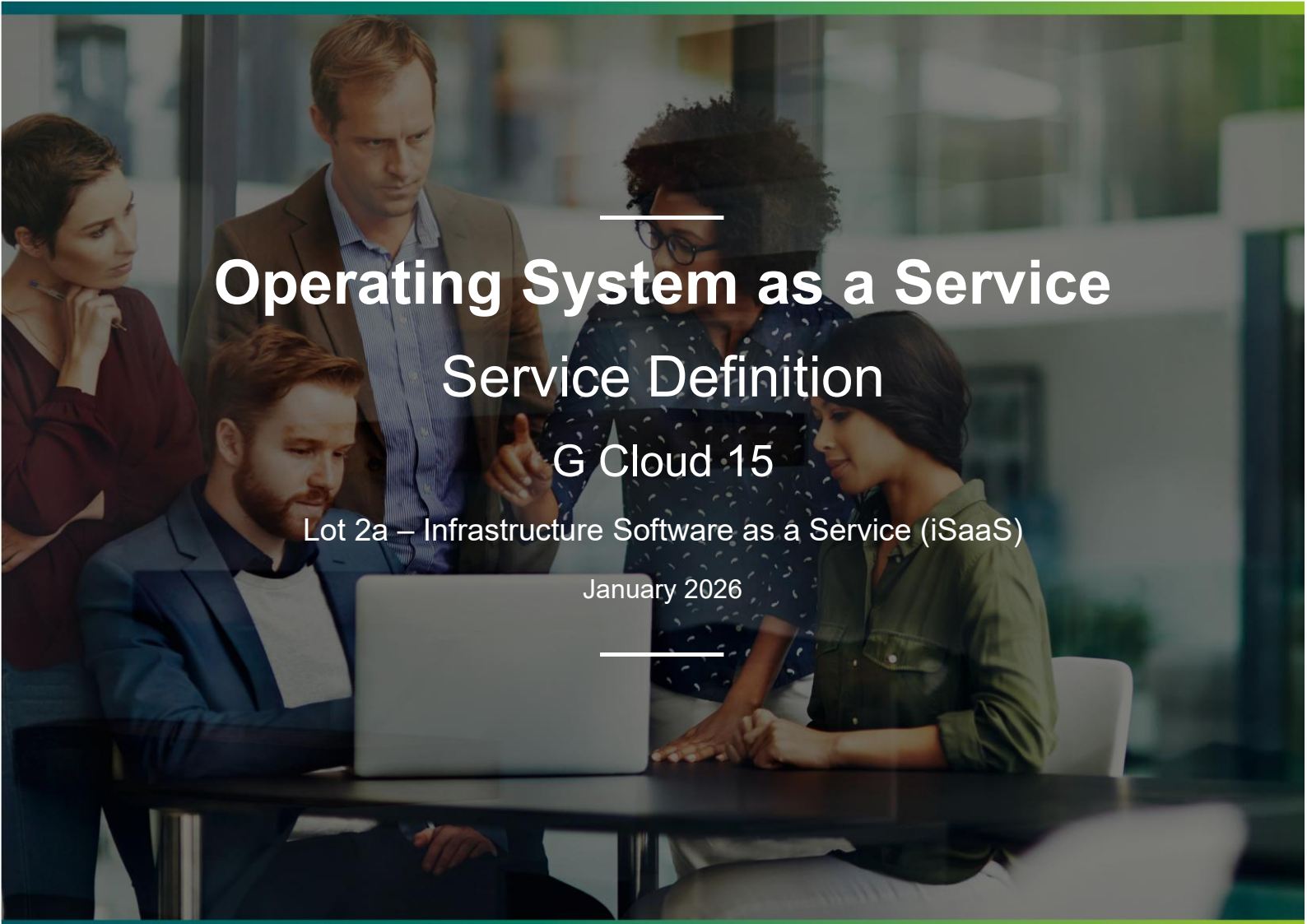




Operating System as a Service

Service Definition

G Cloud 15

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

January 2026

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1.	Service Definition.....	4
1.1.	Key Features	4
1.2.	Key Benefits	4
2.	Scope of Services	5
2.1	Monitoring	5
2.2	Software Agents	5
2.3	Operating System Patching	5
2.4	Anti-Virus	6
2.5	Server Protection	7
2.6	Server Access	7
2.7	Remedial Actions	7
2.8	Software Licensing.....	8
2.9	Server Accounts	8
2.10	Managed Server Location.....	8
2.11	Server Hardening	9
2.12	Operating System Upgrades.....	9
2.13	Service Provisioning	10
2.14	Managed Service as a Service Acceptance.....	10
2.15	Service Restrictions	10
3	Service Attributes & Migration Strategies	12
3.1	Service Transition and Early Life Activities	12
4.	Associated Redcentric Services.....	13
5.	Service Availability	14
5.1	Service Hours Definition.....	14
5.2	Standard Applicable Service Hours.....	14
5.3	Redcentric Service Levels.....	14
6.	Responsibilities and Accountabilities	17
6.1	High Level Redcentric Responsibilities	17
6.2	High Level Customer Responsibilities	17
6.3	RACI Matrix	17
7.	Business Continuity and Disaster Recovery	20
7.1	Business Continuity.....	20
7.2	Disaster Recovery.....	20
8.	Data	22
8.1	Personal Data Processing Statement	22
8.3	Duration of the processing	22
8.5	Categories of Data Subject International Transfers.....	22
8.6	Sub Processors engaged by Redcentric (sub-contractors).....	22

8.7	Types of Personal Data Processed	22
8.8	Special Category Data	22
9.	Exit Plan.....	24
10.	Project management.....	25
11.	Account management	27
12.	Service management	28
13.	Support Services	29
14.	Information assurance	30
15.	Professional services	31
16.	Company profile	32
17.	Why choose Redcentric?	33

1. Service Definition

Redcentric will manage servers provided on the Redcentric Infrastructure as a Service, hosted physical server services, or managed public cloud infrastructure. The service provides access to the Redcentric support capability, technical skills, and economies of scale, to manage a customer's server operating systems.

1.1. Key Features

The Operating System as a Service provides access to Redcentric support capability, technical skills, and economies of scale, to manage the customer's server operating systems deployed on Redcentric managed virtual or physical servers.

The standard service includes:

- Server operating system deployment
- Server operating system customer for all managed servers on the shared platform
- Server monitoring
- Server operating system patching
- Anti-virus deployment and management
- Server availability management

Operating System as a Service will support in support versions of the following OS:

- Microsoft Windows Server - Note this excludes Core and Nano
- Red Hat Enterprise Linux
- CentOS Ubuntu
- Debian

Deployment on virtual or physical servers provided by Redcentric.

Redcentric will deploy the server operating system to a default best practice build on behalf of the Customer, when provisioning a new managed server.

1.2. Key Benefits

- Reduction in customer resource for server administration
- Base level of security/hardening provided as standard
- Access to expertise in server management and troubleshooting
- Proactive monitoring and security
- Assurance of regular updates and patching
- High uptime and reliability
- 24/7 Technical support
- Built in backup and recovery
- Server performance optimisation

2. Scope of Services

This is an optional service to “Redcentric Cloud” and “Redcentric Sovereign Cloud” for existing Redcentric Cloud customers or customers purchasing Redcentric Cloud.

2.1 Monitoring

Redcentric will connect the managed server to a Redcentric server management network using a dedicated network interface. Redcentric will monitor the server using a combination of Simple Network Management Protocol (SNMP) and Windows Management Interface (WMI) for Windows servers.

Redcentric will monitor the managed server for:

Metric	Windows Server & Linux Server
Processor	Alert if processor exceeds a threshold over a set time period
Memory	Alert if memory exceeds a threshold over a set time period
Disk	Alert if usage exceeds a threshold over a set time period
Availability	Alert if the server does not respond to polling requests

Alerts generated by monitoring will automatically raise an incident within Redcentric service desk. Redcentric will investigate the alert and corresponding fault, as detailed in the Remedial Action paragraph below.

Please note that SNMP must be installed and enabled on Linux systems to enable the service, where available SNMP V3 will be configured in preference to older versions.

2.2 Software Agents

Redcentric will install a software agent within managed server operating system for the following functions:

Software function	Windows Server	Linux Server
Antivirus	Agent installed	Agent installed
Patching	Agent installed	OS function
Backup (if taken)	Agent installed	Agent installed
Licence audit	Agent installed	Agent installed
Monitoring	OS function via WMI & SNMP	OS function via SNMP

2.3 Operating System Patching

Redcentric will only apply patches applicable to the managed server operating system. Redcentric will work with the customer during deployment of the managed servers to define patching groups and maintenance windows. Redcentric recommends following best practises and managed servers should be patched regularly, where practical ideally once a month and at most every three months.

The process for applying patches is as follows:

- Redcentric identifies available patches for each managed server and raises all appropriate changes

- Redcentric sends the patching report of patching groups and patches that will be installed on previously agreed date/times
- Customer reviews the patching report and informs Redcentric of any changes required i.e. patches not to be installed
- Redcentric carry out pre-patching activities prior to patching taking place
- Patches are applied and managed servers are rebooted
- Redcentric carry out post-patching checks and update customer on the completion status of the patching

Redcentric will work with the customer to update the patching groups including additions, deletions, and amendments throughout the lifecycle of the service. Keeping managed servers patched and up to date is an essential requirement for the Operating System as a Service.

Please note the following:

- If Redcentric are not informed of any changes to a scheduled patching group within the timescales below it will proceed with the patching
- If a customer wishes not to have any of the automatically approved updates applied, then they must inform Redcentric at least 24 hours before the scheduled start of the patching.
- If a customer wishes to amend a patching groups schedule this must be done 48 hours before the patching is scheduled to take place. If the customer requests changes within the 48-hour period before the patching is scheduled to start, then the patching should be suspended. Once the review has been completed the patching group will be re-scheduled.

Any managed servers that are not patched on a minimum of a three-monthly cycle will not have an associated Service Level Agreement.

Unless Open-Source Operating Systems are subscribed to with a commercial support agreement, bug fixes and patches are subject to release by the Open-Source Community.

Legacy Linux releases can be supported provided a then current Extended Long Term Support agreement is subscribed to.

Redcentric uses several third-party tools to patch Windows and Linux servers. Any additional infrastructure (hardware, licenses etc.) required outside of the standard managed server service to provide patching will be chargeable to the customer.

2.4 Anti-Virus

Redcentric will install, monitor, and manage anti-virus software on each managed server. The anti-virus software used is provided by Sophos and is configured with the following functions:

- On access scanner: Scan executable, known vulnerable and file with no extensions on all drives
- Tamper control: Stop unauthorised configuration changes to the anti-virus software (Windows Server only)
- Device control: Block unauthorised external storage devices and wireless connection and short-range access (Windows Server only)
- Exploit Prevention Model enabled
- Auto update: Check for update virus and malware definitions every 15 minutes

The customer has no administrative access to the anti-virus software; all servers have the same Redcentric defined anti-virus protection. Redcentric will collaborate with the customer to implement the initial file exclusion list as part of the Service Implementation.

Redcentric will terminate the Service Level Agreement (SLA) and not honour associated service credits if the Managed Server Service is affected by the customer's disabling or removing anti-virus software.

2.5 Server Protection

Redcentric will protect the managed server, when delivered as a virtual server on Redcentric Infrastructure as a Service, for the purposes of Redcentric being able to restore to an earlier working point if required as part of fault finding.

Server protection for physical servers will be done through a daily back up (remote of the system volume (OS) only, performed each night, and retained for 7 days, onsite to the managed server.

Server protection for virtual servers will be by storage snapshots (full server) performed each night, and retained for 7 days

Server protection is not a substitute for customer performed backups as it does not provide:

- Granular file restoration
- Self-service access to the customer to restore data
- Data retention beyond 7 days
- Offsite storage of backup data
- Redcentric can provide a managed backup service to complement Operating System as a Service

2.6 Server Access

Redcentric allows the following access to the managed server.

Access method	Description
Console access	The managed server console can be accessed by a RDP (Remote Desktop Protocol) session to a Windows server, or a SSH (Secure Shell Protocol) session to a Linux server.

2.7 Remedial Actions

Redcentric will perform remedial actions on the managed server where a fault is identified through monitoring. The objective of the remedial actions is to re-instate the managed server to a working state that includes:

- Managed server responding to monitoring agent
- Managed server monitored counters all below the alert trigger thresholds
- Managed server disks not full
- All automatic services running

To return the managed server to a working state, Redcentric will perform the following remedial actions:

- Notify the customer upon detecting a fault with the managed server
- Investigate the fault and identify what steps are required.

This could include:

- Remove temporary files
- Expand disk space
- Restart the managed server if the server is unresponsive
- Restore the managed server from a previous protection point

Co-ordinate remedial actions with the customer, specifically where it is identified that a customer application is at fault. If necessary, a rebuild to the managed server may be required to a default install.

During out of hours periods, unless a server is unresponsive, Redcentric will record that the server is outside of normal operating parameters but will not intervene. If a critical threshold is reached Redcentric will contact customer personnel to agree remediation steps and intervene as directed.

A critical event is defined as:

- Filesystem utilisation exceeds 94% (except where applications have pre-allocated space)
- CPU usage is sustained at 100% for 1 hour or more (exclusions for backup windows may apply)
- RAM usage exceeds 90% for a sustained period of 15 minutes or more (except where applications allocate all available RAM when working as designed)

2.8 Software Licensing

Managed Service as a Service includes the following software licences:

- Operating system licences for all managed servers on the shared platform
- Sophos anti-virus to be installed on the managed server (shared and dedicated hardware)
- Monitoring software used by Redcentric

Customer application licences are not included within Managed Service as a Service but can be provided as a separate licence charge via the Redcentric service provider licence agreements. Or under certain circumstances customers may utilise their own licences under a licence mobility agreement.

Operating System (OS) licences for managed servers on dedicated hardware can utilise the customer's existing licences or they can be provided as a separate chargeable item by Redcentric.

Customers migrating from an unmanaged service to the shared service will use Redcentric licences.

2.9 Server Accounts

Each managed server will be created in non-domain joined mode with local user and group accounts by default. The managed server can be deployed within an existing customer domain if available.

To operate this Service Redcentric is required to have an administrator level account on the server for management and licence audit purposes.

2.10 Managed Server Location

Redcentric will provide Managed Service as a Service on servers provided on either the Redcentric Infrastructure as a Service (IaaS) hosted physical server services or Managed Public Cloud (AWS/Azure) Services. For IaaS and hosted servers, the managed servers will be provided on equipment from within Redcentric UK data centres. No access will be provided to the underlying physical infrastructure for monitoring, reporting or third-party hardware installations i.e., USB devices.

Where a Managed Public Cloud (AWS/Azure) Service is subscribed to, Health monitoring of the Public Cloud infrastructure supporting the Managed Virtual Machines will be established and available to customers.

2.11 Server Hardening

The goal of hardening a system is to remove any unnecessary functionality and to configure what is left in a secure manner. Every application, service, driver, feature, and setting installed or enabled on a system can introduce vulnerabilities, especially if left at default settings.

However, there is no one size fits all solution – whilst there are guidelines/recommendations from bodies such as CIS (Centre for Internet Security) these are just a suggestion, and each customer/application may have specific requirements that can only be identified during the contract build/on-boarding phase. The Redcentric pre-sales team will collaborate with customers to provide advice on hardening as required during the sales process.

Server hardening is available for customers on dedicated or shared hardware who are using Windows Server 2016 and later releases. At the start of a contract a customer can choose either a standard or hardened OS. Both the standard and hardened OS are the same price at the start of a contract.

Redcentric provide both hardened and standard OS images for Linux.

The recommended approach for customers requiring hardened images is to start with a Centre for Internet Security (CIS) aligned build and then soften the security posture only when it is preventing the application from operating correctly. This aligns with the authorisation best practice to apply the least privilege principle,

If a customer initially chooses a standard OS and then at any point from initial deployment onwards decides to change to the hardened version a One-Off Professional Services Charge from Operating System as a Service Price Card will apply.

2.12 Operating System Upgrades

Redcentric will patch the server for the purposes of security and keeping it within a vendor supported level.

For major operating systems upgrades, for example Windows Server 2012 to Windows Server 2016, Redcentric default approach is to provision a new server along the existing server, and allow the Customer to transfer applications, configuration, and data. Provisioning new servers may incur an additional charge in the following cases:

Hosted Private Cloud – Typically customers will utilise spare capacity within a dedicated platform, but if additional Hosted Private Cloud hosts are required a charge will be incurred for the platform upgrade.

Infrastructure as a Service – This is a usage service and additional servers will incur an additional Charge.

Hosted Physical Servers – A new Hosted Physical Server will be required to host the upgraded operating system.

Redcentric can perform in-place operating system upgrades by exception to the above. This will incur an additional Charge to cover the plan, test and implement activities. It is expected that in-place upgrades will be performed out of hours for production customer workloads.

2.13 Service Provisioning

Redcentric will deploy new managed servers as part of the Service delivery. By default, this will include:

- Deployment of a managed server from a Redcentric template
- Patching to the latest available patch level
- Installation and configuration of anti-virus software
- Creation of a configuration item with Redcentric configuration management database
- Setup of server monitoring
- Setup of server protection schedule
- Creation of local user accounts and groups
- Acceptance of the server into monitoring and support

Upon Service activation, the customer will be able to access the managed server to install their applications. Additionally, the customer can engage Redcentric Professional Services to:

- Design and deploy Microsoft active directory domain for the managed servers
- Design and deploy Redcentric Backup as a Service

The target lead time to complete Service Delivery is detailed in the table below, for each Service element. This is subject to the timescales of delivery of the specific connection mechanism used to connect the customer to Managed Service as a Service, such as delivery of Ethernet access circuits, NHS HSCN connection, Internet address allocation via RIPE (Regional Internet Registry for Europe, Middle East and Central Asia), firewall configuration, options selected, etc.

Service Element	Service Activation Timescales
Service Implementation	Target completion within 20-working days

2.14 Managed Service as a Service Acceptance

The following are the Acceptance Criteria applicable to Managed Service as a Service:

- Verify that the primary customer contact can access the managed server
- The customer will nominate (pre-installation) and make available an appropriately qualified representative to work with the Redcentric representative during the service delivery. The nominated customer representative will accept delivery of Managed Service as a Service as a fully commissioned service and sign the service sign-off document and return this to Redcentric. The installation will be conducted between 09:00 to 17:30, Monday to Friday, unless otherwise agreed.

2.15 Service Restrictions

The following are excluded from the scope of Managed Service as a Service.

- Reporting on performance metrics
- Backup or disaster recovery to a second data centre
- Patching of customer applications not included within the Microsoft Windows update or Linux yum repositories
- Licensing of customer applications
- Licensing of the operating system for managed servers on dedicated hardware is an option that the customer can pay for, but is not provided by default
- Support of the customer applications
- Backup of the customer data to a second data centre, unless taken as part of a separate Redcentric service

- Recovery of the customer managed server to a second Redcentric data centre, unless taken as part of a separate Redcentric service
- Deleting files, other than temporary files, as part of remedial actions
- Active directory domain management (Windows Server only)
- LDAP system management
- Existing customer server deployments cannot be brought into the scope of Managed Service as a Service.

3 Service Attributes & Migration Strategies

3.1 Service Transition and Early Life Activities

Onboarding will include:

- Managed server deployment from a Redcentric template
- Patching to latest available patch level
- Anti-virus software Installation/configuration
- Creation of a configuration item with Redcentric configuration management database
- Monitoring setup
- Server protection schedule setup
- Local user accounts and groups creation
- Acceptance into monitoring and support

Redcentric will collaborate with the customer to define patching groups and maintenance windows. Redcentric will protect the managed server, when delivered as a virtual server on the Redcentric Infrastructure as a Service, for the purposes of Redcentric being able to restore to an earlier working point if required as part of fault finding.

Each managed server will be created in non-domain joined mode with local user and group accounts by default. The managed server can be deployed within an existing customer domain if available.

The customer will nominate (pre-installation) and make available an appropriately qualified representative to work with the Redcentric representative during the service delivery. The nominated customer representative will accept delivery of Managed Service as a Service as a fully commissioned service and sign the service sign-off document and return this to Redcentric.

Upon Service activation, the customer will be able to access the managed server to install their applications.

4. Associated Redcentric Services

The table below provides details of other compatible services available from Redcentric via G-Cloud 15.

Service Name	Service Summary
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"
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"
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.
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.
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.
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.
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.

5. Service Availability

5.1 Service Hours Definition

There are two (2) levels of Redcentric service hours, defined as follows.

Service Hours Description	Definition
24x7x365	Available 24 hours a day, 7 days a week, 365 days a year.
Redcentric UK business hours (PBH)	09:00 am to 17:00 pm GMT / BST (as applicable) Monday to Friday excluding UK public holidays

5.2 Standard Applicable Service Hours

Service Management Activity	Service Hours
Redcentric Service Desk	24x7x365
Support Request Management	Redcentric UK business hours
Incident Management (P1)	24x7x365
Incident Management (P2 & P3)	Redcentric UK business hours
Problem Management (RCA)	Redcentric UK business hours
Configuration Management	Redcentric UK business hours

The management of support requests (covering requests for information, ticket updates and request for change) will be provided within Redcentric business hours, to ensure the quality of the communication channels.

More specific aspects of service management, such as root cause analysis where the underlying cause of an incident is not yet identified – known as a problem – and the management of change and releases are also conducted within Redcentric business hours to ensure the rigorous and effective delivery of these service elements.

5.3 Redcentric Service Levels

The Service Level applicable to Managed Service as a Service is as follows:

Service Level	Measurement Period
Availability	Month. Not less than the Service Level applicable to the underlying service on which Managed Service as a Service is provided

The following exclusions apply:

- Outages that are caused by OS bugs where no fix exists
- Outages that occur when a work-around or patch has been identified that has been notified to the customer but have not yet been implemented

5.4. Floor Service Level

The Floor Service Level applicable to Managed Service as a Service in respect of Availability shall be 85% in any given Month.

5.5. Service Credits

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

$$\text{Service Credit} = \frac{C \times S}{MS}$$

Where:

S = the number of seconds by which Redcentric fails to meet the Service Level for Availability in the relevant Month

C = total Charges payable in respect of Managed Service as a Service for the same Month

MS = the total number of seconds in the same month

5.6. Restoration Targets

Redcentric standard restoration times for each incident priority level are shown below, all hours are based on the geography of the customer location.

An incident will be assigned to the most appropriate team for resolution. Throughout the resolution process, the Incident will be updated to indicate progress.

Target Resolution relates to any item within Redcentric control to resolve. Where a service issue is related to a third-party service Redcentric will raise all appropriate tickets and/or escalations with relevant vendor (e.g. Microsoft Azure) if the relationship is directly with Redcentric (applicable to Operate & Modernise service tiers). In this case, the vendor's terms of service/condition apply for incident resolution.

Priority	Definition	Target Resolution	Hours in Effect
P1	A system or application is down and defined as critical by the customer. The system/application has a material impact on the ability to carry out business as usual	4 hours	24 x 7 x 365
P2	A non-critical system or application that is being affected or down to such a degree as to impede business as usual	8 hours	Mon to Fri 08:00 – 18:00
P3	An issue affecting services that is not business critical	36 hours	Mon to Fri 08:00 – 18:00
P4	A non-business impacting event requiring investigation	5 business days	Mon to Fri 08:00 – 18:00

5.7. Escalation Management

The Redcentric ITSM system will monitor the lifecycle of an incident according to its priority. An incident can be escalated for two main reasons:

- Technical (or functional) escalation is the process of re-assigning an incident from one team to another based on the skills required to resolve the incident; and
- Management (or hierarchical) escalation refers to the involvement of increasing senior levels of management in the efforts to resolve an incident.

5.8. Problem Management

In the context of IT services, a problem is indicated where the root cause of an incident is unknown. In this scenario, normal service may be restored by means of a temporary work-around rather than

waiting for a lengthy investigation. A problem may also be indicated if multiple incidents exhibit the same symptoms.

Redcentric has implemented Problem Management to manage the following activities:

- Identification of the underlying causes of incidents
- Evaluation of the impact of recurring incidents
- Targeting the elimination of underlying causes where appropriate.

5.9. Change Management

The goal of Change Management is to ensure that standard procedures are used for efficient and prompt handling of all changes. This minimises the impact of change-related incidents on service quality and consequently improves the day-to-day operations of an organisation.

All requests for change will be managed in line with accepted ITIL principles to ensure their potential risk is properly addressed. Redcentric will evaluate each request for change using a combination of impact and urgency. The change category determines the target time for completion of a change as shown in the following table:

Change Category	Target Completion Time
Emergency e.g. high priority changes required to rectify or prevent a P1 incident.	Up to 48 hours
Normal e.g. significant changes where scheduled downtime is most likely required to implement resolution.	by agreement following review of change requirements
Standard Changes where the customer has pre-approved the implementation process (such as documented software patches). Standard changes can be handled as a Service Request without formal Change Management approval.	2 to 7 working days

6. Responsibilities and Accountabilities

6.1 High Level Redcentric Responsibilities

Redcentric standard service includes:

- Server operating system deployment
- Server operating system customer for all managed servers on the shared platform
- Server monitoring
- Server operating system patching
- Anti-virus deployment and management
- Server availability management

6.2 High Level Customer Responsibilities

The customer will:

- The following are customer dependencies for Managed Service as a Service.
- Provide a patching maintenance window for the managed server that includes a reboot if required
- Review and, if necessary, reject, patches to be applied to the managed server operating systems. Patch notification automatically generated 1 week before the agreed patching maintenance window
- Install, configure, license, and manage applications used on the managed server, such as IIS, Apache, DNS, MySQL, WINS, DHCP, etc.
- Define anti-virus exclusions required for the customer applications
- Allow Redcentric administrator level account on the managed server during the life of the service

6.3 RACI Matrix

The following table outlines Redcentric and customer responsibilities using a RACI model.

- Responsible: Do the task
- Accountable: Approve the task
- Consulted: Input provided to the task
- Informed: Notified on task progress or completion

Task	Customer	Redcentric
Managed server administration		
Operating system support	I	R, A
Day to day support / maintenance and incident resolution of each managed server	I	R, A
Deployment of new managed servers at the request of the customer	C	R, A
Implementation, configuration, and maintenance of monitoring agent	I	R, A
Implementation, configuration, and maintenance of local server protection	I	R, A

Task	Customer	Redcentric
Storage management		
Disk management	I	R, A
Storage area network (SAN) / network area storage (NAS) management (if applicable)	I	R, A
Backups		
Install, operate, and manage backup infrastructure	R, A	I
Ensure backup jobs are set up according to policy	R, A	I
Data restoration, such as individual files requests from end-users	R, A	I
Disaster recovery	R, A	I
Patching		
Review and assessment of available patches for managed servers and recommend to Customer which patches should be applied	C	R, A
Approval of managed server patch implementation plan	R	I
Execution of managed server patch implementation plan	C	R, A
Provide patch distribution infrastructure (e.g. Microsoft WSUS / yum repository)	C	R, A
Monitoring		
Specify/confirm monitoring alarm thresholds	C	R, A
Specify/confirm critical monitoring alarm thresholds	R	I
Implementation of monitoring agents and out-of-band data collectors	I	R, A
Monitoring of alarms	I	R, A
Capacity planning		
Own the capacity planning of the managed server	R, A	I
Identify potential performance bottlenecks for discussion at the service review	R, A	C
Discuss capacity change options	R, A	C
Approving capacity change options	R, A	I

Task	Customer	Redcentric
Implement identified capacity recommendations	C	R, A
Administration of user access and permissions		
Creation/management of administrative user accounts for access to managed server	I	R, A
Request additional user access to the managed server	R, A	I
Availability management		
Monitor managed server availability	I	R, A
Perform analysis where availability triggers a monitoring alert	I	R, A
Remediate managed server to make managed server available	I	R, A
Anti-virus management		
Installation, configuration, monitoring, and management of anti-virus software	I	R, A
Application management		
Installation, configuration, licensing, monitoring, and management of application software	R, A	I

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 as a 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 is designed and engineered to deliver highly available, stable connectivity to maintain business access to critical applications. To maximise resilience, multiple carriers provide core connectivity and routing, and switching devices are 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

As part of the service Redcentric will take daily backups of

1. Server OS
2. Application
3. Files and Data
4. Server configuration

This back will then be available to the customer to restore the server in the event of corruption or failure. This service is compatible with the Redcentric Disaster Recovery as a Service which would provide the customer with a managed disaster recovery service. Redcentric can also provide target infrastructure to support disaster recovery.

In terms of Redcentric internal services that support this service, Disaster Recovery plans underpinning the BCP have been developed for each Department and Service, and these are externally audited and tested annually.

8. Data

8.1 Personal Data Processing Statement

Note that in completion of this Statement, the Customer is the Controller and Redcentric is the Processor unless otherwise stated.

8.2 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 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.

It will be necessary to store Customer commercial users' personal data to manage the Account and provide Service, and to raise invoices.

The solution, service desk provision and data back-up facilities are in Data Centres in the UK unless otherwise stated. Redcentric also provides monitoring, management, back up, incident resolution and reporting.

The legal basis for the processing is to satisfy the obligations contained within the Customer Contract.

8.3 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.

8.4 Categories of Data Subject

Customer Commercial, Account, Technical, and Finance personnel.

8.5 Categories of Data Subject International Transfers

It may be necessary for our Support operation in Hyderabad to access personal data to authenticate 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

The following data is processed:

- Customer Administrator details (Username, First and Last names, email address, Job Title).
- Customer Commercial and finance details (First and Last names, email address, Job Title).

8.8 Special Category Data

No special category data is accessed by Redcentric personnel.

8.9 Data Processing Location

- UK

- EEA (EU)
- Adequate Country (UK, US; (commercial organisations participating in the EU-US Data Privacy Framework), Canada, Israel, others)
- International Data Transfer Agreement in place (Redcentric India)

9. Exit Plan

At the Call-Off Contract end date, the service will cease. All software associated with the delivery of the service will be removed from the servers. The servers will be removed from any scheduled updates and patches. Access to the service by red centric engineers will be removed restricted two engineers involved in the delivery of residual services not associated with Managed Server as a Server.

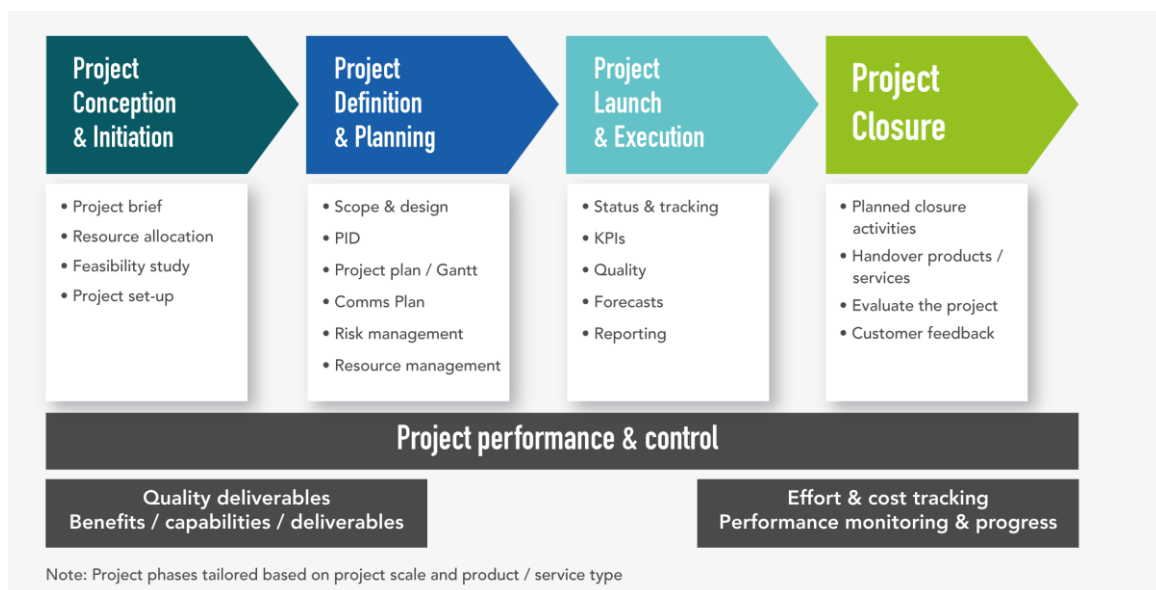
10. Project management

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

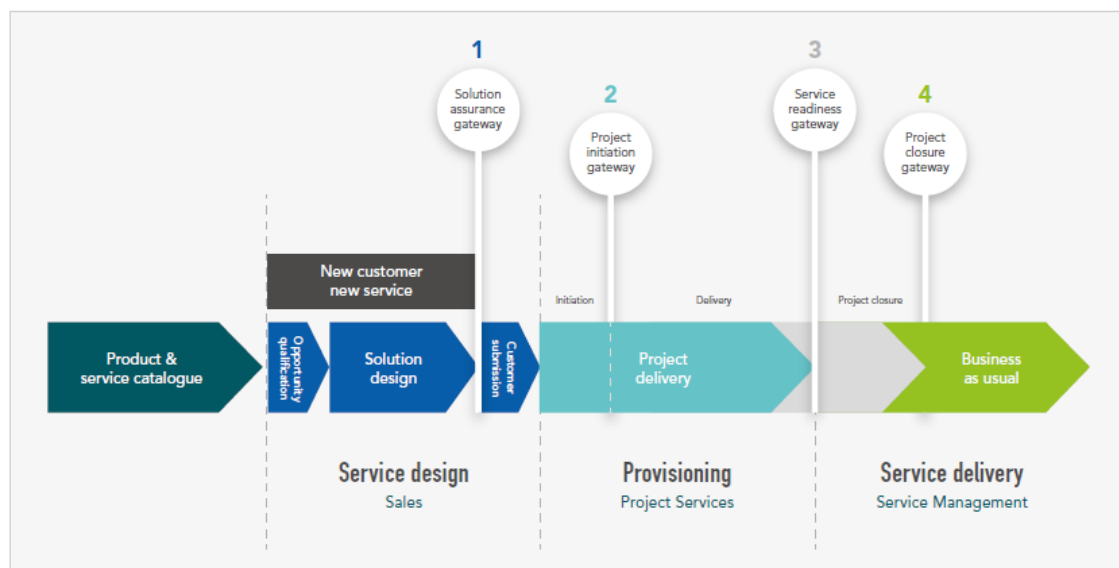
- Test plan to minimise disruption to your business operations
- Communications plan that defines what information to share and with whom
- Site implementation tracker to record the migration progress
- Weekly highlight report providing project updates
- Customer Service Pack
- UAT Test Report – per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

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:

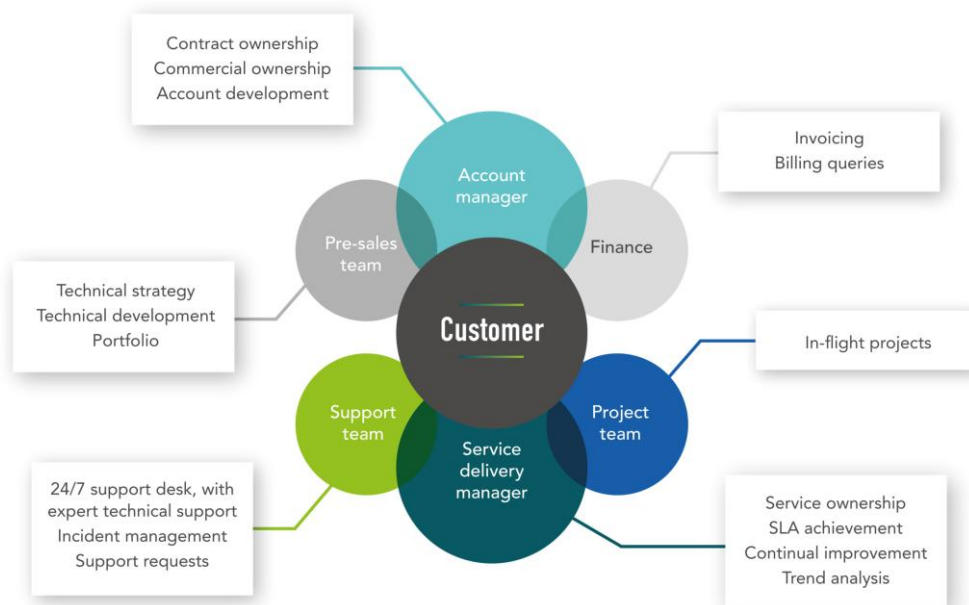
- Technical delivery is achieved on time and to specification
- The support model is fit for purpose and available at service commencement
- You will experience a 'soft landing' with minimal disruption to service.



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.



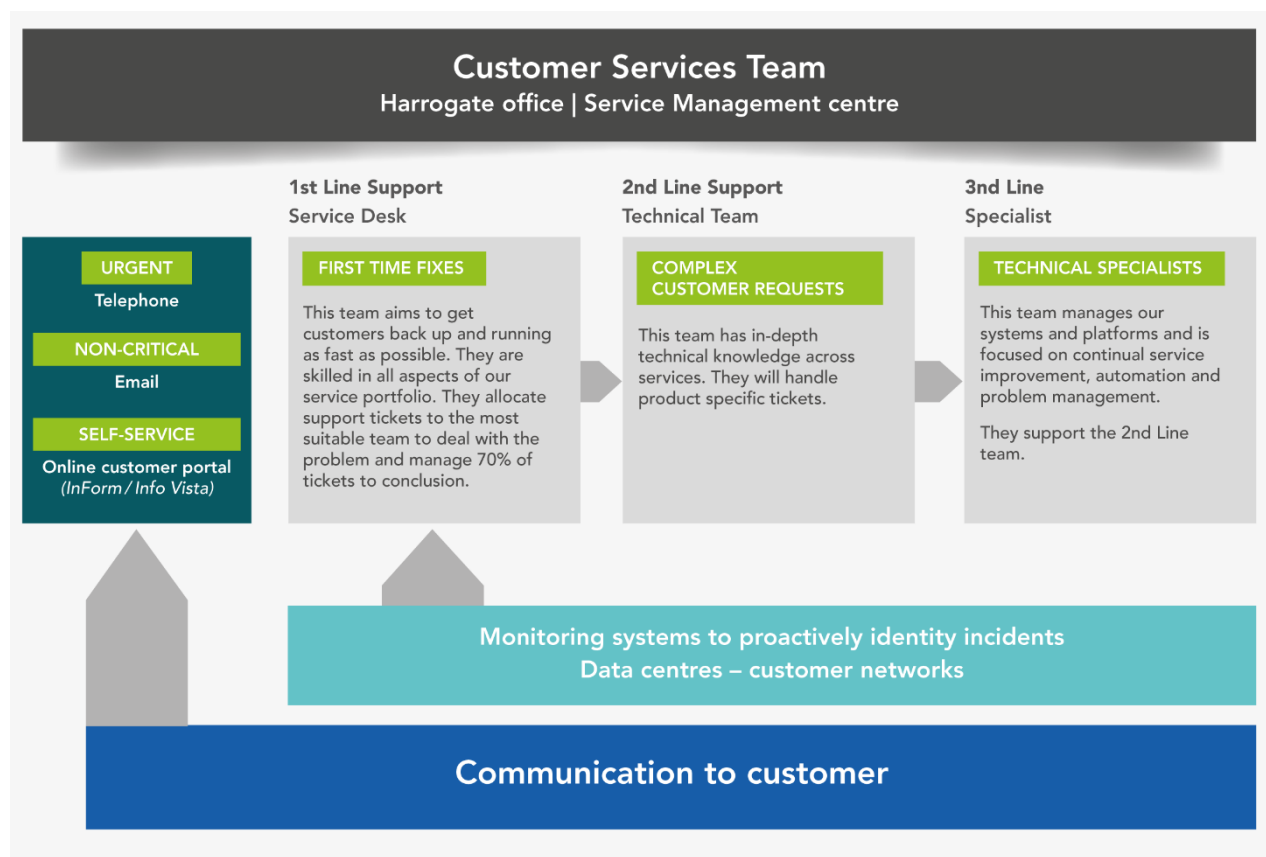
We have thoroughly documented the major incident and customer service plans, which detail how we operate in business-as-usual scenarios and during major incidents.



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

