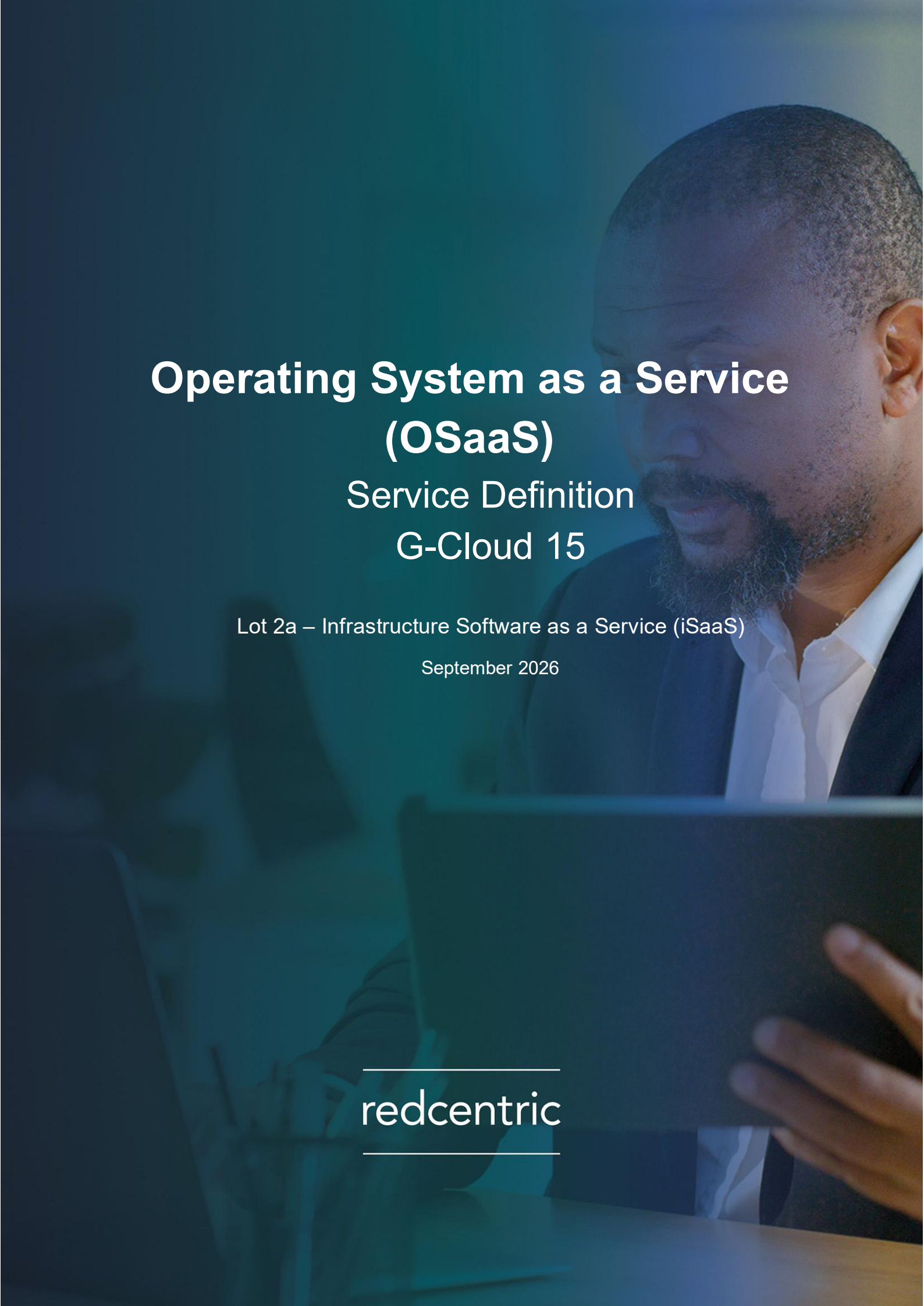




Operating System as a Service (OSaaS)

Service Definition
G-Cloud 15

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

September 2026

redcentric

Contents

1.	Service Definition	3
1.1	Key Features	3
1.2	Key Benefits.....	3
1.3	Monitoring	4
1.4	Software Agents	4
1.5	Operating System Patching	4
1.7	Server Protection.....	6
1.8	Server Access	6
1.9	Remedial Actions	6
1.10	Software Licensing	7
1.11	Server Accounts	7
1.12	Managed Server Location	7
1.13	Server Hardening	8
1.14	Operating System Upgrades.....	8
1.15	Service Provisioning	9
1.16	Operating System as a Service Acceptance.....	9
1.17	Service Restrictions	10
2.	Onboarding and Offboarding	11
2.1	Migration Support	11
2.2	Onboarding	11
2.3	Service Delivery Management.....	12
3.	Service Levels.....	14
3.1	Service Hours Definition	14
3.2	Applicable Service Hours.....	14
3.3	Service Levels	14
4.	Responsibilities	16
5.	Associated Services	17
6.	Business Continuity and Disaster Recovery	18
7.	Data Management.....	20
8.	Information Assurance.....	22

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.

This is a complementary service to "Redcentric Cloud" and "Redcentric Sovereign Cloud" for existing Redcentric Private or Public Cloud customers or customers purchasing Redcentric Cloud.

1.1 Key Features

The Operating System as a Service provides access to Redcentric's 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 monitoring
- Server operating system patching
- Anti-virus deployment and management
- Server availability management

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

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

Deployment is available 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

1.3 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 following:

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 to the 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, SNMPv3 will be configured in preference to older versions.

1.4 Software Agents

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

Software function	Windows Server	Linux Server
Anti-virus	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

1.5 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 practices and managed servers should be patched regularly, where practical, ideally once a month and as a minimum 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 dates and times
 - The customer reviews the patching report and informs Redcentric of any changes required, i.e., patches not to be installed
 - Redcentric carries out pre-patching activities prior to patching taking place
 - Patches are applied and managed servers are rebooted
 - Redcentric carries out post-patching checks and updates the 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 is 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 group's 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 rescheduled.

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.

1.6 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 files and files 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 connections and short-range access (Windows Server only)
- Exploit prevention module enabled
- Auto update: Check for updated 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.

1.7 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 it to an earlier working point if required as part of fault finding.

Server protection for physical servers will be done through a daily backup of the system volume (OS) only, performed each night, and retained for seven days.

Server protection for virtual servers will be by storage snapshots (full server) performed each night, and retained for seven 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 seven days
- Offsite storage of backup data
- Redcentric can provide a managed backup service to complement Operating System as a Service

1.8 Server Access

Redcentric allows the following access to the managed server:

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

1.9 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 reinstate 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.

These 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

Coordinate 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 the customer's 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)

1.10 Software Licensing

Operating System as a Service includes the following software licences:

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

Customer application licences are not included within Operating System as a Service but can be provided as a separate licence charge via the Redcentric service provider, 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 from the Redcentric Cloud service.

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

1.11 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.

1.12 Managed Server Location

Redcentric will provide Operating System as a Service on servers provided on either the Redcentric Infrastructure as a Service (IaaS), hosted physical server services or managed public cloud (Azure/AWS) services. For IaaS and hosted servers, the managed servers will be provided on equipment from within our partner UK data centres. No access will be provided to the underlying physical infrastructure for monitoring, reporting or third-party hardware installations, for example 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.

1.13 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 – while there are guidelines/recommendations from bodies such as CIS (Centre for Internet Security), these are suggestions, and each customer/application may have specific requirements that can only be identified during the contract build/onboarding 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 provides 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 the Operating System as a Service catalogue price will apply – see section 6, Catalogue Price, for details.

1.14 Operating System Upgrades

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

For major operating system upgrades, for example Windows Server 2012 to Windows Server 2016, Redcentric's default approach is to provision a new server alongside 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 – see our Redcentric Cloud service (RM6190-L4-RSL011) for details.

Infrastructure as a Service – This is a usage-based service and additional servers will incur an additional charge - see our Redcentric Cloud service (RM6190-L4-RSL011) for details.

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 professional services charge to cover the planning, testing and implementation activities – see section 6, Catalogue Price, for details. It is expected that in-place upgrades will be performed out-of-hours for production customer workloads.

1.15 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 within Redcentric's configuration management database
- Configuration of server monitoring
- Configuration of the 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 a 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 Operating System 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

1.16 Operating System as a Service Acceptance

The following are the acceptance criteria applicable to Operating System as a Service:

- Verify that the primary customer contact can access the managed server
- The customer will nominate (before installation) and make available an appropriately qualified representative to work with the Redcentric representative during service delivery. The nominated customer representative will accept delivery of Operating System 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 and 17:30, Monday to Friday, unless otherwise agreed.

1.17 Service Restrictions

The following are excluded from the scope of Operating System as a Service:

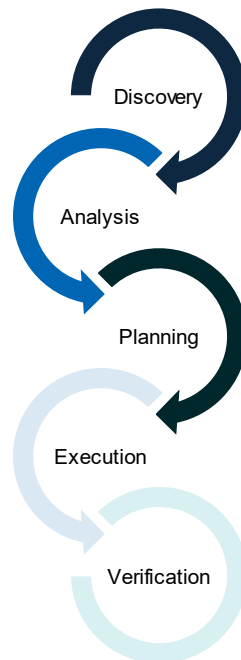
- Reporting on performance metrics
- Backup or disaster recovery to a second data centre
- Patching of customer applications not included within the Microsoft Windows update or Linux yum repositories
- Licensing of customer applications
- Licensing of the operating system for managed servers on dedicated 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 Operating System as a Service.

2. Onboarding and Offboarding

2.1 Migration Support

Migration support is available as an additional service component charged as a one-off professional services charge. There are options for fully managed and joint migrations, with support from the customer, which will be reflected in the price.

Migrations are delivered using a standard five-stage methodology as shown below.



2.2 Onboarding

The following sections provide information on what customers should expect to receive from Redcentric as part of their onboarding. It is intended as a high-level guide to help customers understand what is required to ensure the delivery of a successful service and covers customer responsibilities as well as the responsibilities of Redcentric.

During the design phase, service onboarding will cover the following activities:

- An introductory meeting, run by the Redcentric Service Delivery Manager (SDM) allocated to the customer's account.
- Engagement with the Redcentric Service Management team to explain how the customer will be onboarded, and what service management functionality and processes will be applied, and what information will be needed to set up the various Redcentric systems, SMAX and My Services portal correctly.
- How service engagement will work, for example, will individual sites be logging issues/requests directly with Redcentric or will there be a centralised first line triage function within the customer's organisation.
- If there is a requirement to implement a B2B link between Redcentric and the customer's ITSM systems, and how this will be implemented.

- Provision of collateral which will enable the customer to communicate the above processes internally.

The Redcentric Transition Programme Governance process provides a series of quality gateways from the perspective of operational support and service management, to facilitate a seamless transition of services from the customer's existing provider to Redcentric. The governance framework provides three quality gateways with standardised criteria against which the project is reviewed, before being approved to proceed to the next phase. There is also a further gateway prior to project initiation, which ensures a smooth handover into project services.

The onboarding responsibilities outlined will be agreed and may vary depending on the hosting model in place (i.e. whether Redcentric or customer-hosted, which may change responsibility for some required tasks).

Redcentric will align a project manager, either dedicated for OSaaS implementation or as part of a wider managed service project, to run a project kick-off, create a project plan, align resources and track progress against the agreed timescales. The customer is responsible for certain activities or the provision/agreement of certain prerequisites to permit delivery of OSaaS, as described below. Before commencement of Redcentric OSaaS, the following transition tasks must be completed:

Responsibilities	
Redcentric	Customer
<ul style="list-style-type: none"> • Implement the Redcentric standard services toolset (e.g. monitoring). • Compile support documentation. • Align a Redcentric support engineer to act as a single point of contact for the purposes of the transition activities. • All System Administration (SA) access to instances that are to be transitioned is removed/downgraded to the least required privilege. • Only the Redcentric support team should have SA access. 	<ul style="list-style-type: none"> • Assign one point of contact to work with Redcentric during transition. Such points of contact shall be authorised to make decisions required for the transition plan activities to proceed.

2.3 Service Delivery Management

Service delivery management is the overarching management of the end-to-end contractual deliverables of the business-as-usual (BAU) service.

Redcentric will designate a Service Delivery Manager (SDM) to act as the primary liaison between the customer and Redcentric operational, architectural, and commercial functions. The SDM will be responsible for the following:

2.4 Scope inclusions

The scope of service delivery management includes the following activities:

- In the event of a hierarchical service escalation, work with the service desk and operations team to ensure BAU service is restored.
- Own any deficiencies in service and act on new requirements that would modify the contract.

-
- At regular intervals, measure how satisfied a customer is with Redcentric services and use trends shown by this information to manage service levels.

2.5 Schedule and facilitate service review meetings

Service review meetings will be conducted remotely via a web collaboration tool (e.g. Teams), or at the customer site, covering the following:

- Review and discuss KPI performance
- customer satisfaction
- service enhancements

2.6 Standard service review reporting

- Telephone/remote support - all support/managed services are delivered remotely unless onsite engineering is contracted separately.
- 24x7x365 service desk
- Access to the Redcentric ITSM platform and L1 Service Desk Analysts for first line fix or resolution.

3. Service Levels

3.1 Service Hours Definition

There are two 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 to 17:00 GMT / BST (as applicable) Monday to Friday excluding UK public holidays

3.2 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 requests 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 carried out within Redcentric business hours to ensure the rigorous and effective delivery of these service elements.

3.3 Service Levels

Target availability for the Redcentric services underpinning the customer's services.

Service	Target Service Level	Definitions
Redcentric Service Desk	99.999%	Service Desk availability to raise support requests.

Target figures relate to availability of the service platform and exclude outages related to single points of failure, scheduled downtime, or those service elements outside of the Redcentric scope of responsibility.

Platform/infrastructure availability is measured by Redcentric's chosen monitoring and event handling tools and the Redcentric POM reporting platform. Redcentric does not include as standard the monitoring of end-user perception of availability or performance, which can be affected by the service quality of the ISP or customer LAN.

The service availability target is defined as the percentage of time for which the service is available to users.

Service availability = ((Agreed service hours – service downtime hours) / agreed service hours) × 100%

Notes:

- All availability targets are to be calculated on a rolling 12-month basis.
- Availability calculations will exclude outages where root cause is determined to be outside of the platform components under Redcentric control.

4. Responsibilities

4.1 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 of task progress or completion

Task	Redcentric	Customer
Provide business and technical requirements	C, I	R, A
Create customer proposal, pricing, and contract documentation	R, A	C, I
Design review	R, A	C, I
Create pre-sales solution and HLD	R, A	C, I
Final proposal to customer	R, A	C, I
Contract signature	C, I	R, A
Manage implementation activities	R, A	C, I
Build/provision the solution	R, A	C, I
Test and handover	R, A	C, I
Notify the customer of any service-affecting issues or planned maintenance	R, A	C, I
Notify Redcentric of any planned activities that may impact service	A, C, I	R
Resolve incidents and problems	R, A	C, I
Raise service requests and changes	C, I	R, A
Implement service requests and changes	R, A	C, I

5. Associated Services

The table below provides details of other compatible services available from Redcentric on 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. It delivers virtualised server, storage and network infrastructure using an OpEx-based consumption model. The platforms are managed by Redcentric covering performance, capacity, patching, installation, and upgrades for data marked "Official" .
Redcentric Sovereign Cloud	Redcentric Sovereign Cloud is a community cloud solution for consumption by UK public sector organisations. It delivers virtualised server, storage and network infrastructure through discrete public sector networks using an OpEx-based consumption model. The platforms are managed by Redcentric covering performance, capacity, patching, installation, and upgrades for data marked "Official-Sensitive" .

6. Business Continuity and Disaster Recovery

6.1 Business Continuity

Redcentric, under its ISO 22301:2019 Business Continuity certification, operates and maintains a robust Business Continuity Management System (BCMS). The BCMS scope includes:

- Data centres
- Managed services
- ICT technologies and systems
- Staff and business functions

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

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

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

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

Testing

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

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

Network Resilience

Our network 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 endpoints).

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 reroute around a failed transit path in under a second.

6.2 Disaster Recovery

As part of the service, Redcentric will take daily backups of:

1. Server OS
2. Applications
3. Files and data
4. Server configuration

This backup will then be available to the customer to restore the server in the event of corruption or failure. This service is compatible with 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.

7. Data Management

7.1 Personal Data Processing Statement

Note that for the purposes of this statement, the customer is the controller and Redcentric is the processor unless otherwise stated.

7.2 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, provide the service and raise invoices.

The solution, service desk provision and data backup facilities are in data centres in the UK unless otherwise stated. Redcentric also provides monitoring, management, backup, incident resolution and reporting.

The legal basis for the processing is to satisfy the obligations contained within the customer contract.

7.3 Duration of the processing

Processing will continue 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.

7.4 Categories of data subject

customer commercial, account, technical, and finance personnel.

7.5 International transfers involving data subjects

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 and telephone number, which may be checked against a pre-approved list.

7.6 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.

7.7 Types of personal data processed

The following data is processed:

- customer administrator details (username, first and last names, email address and job title).
- customer commercial and finance details (first and last names, email address and job title).

7.8 Special category data

No special category data is accessed by Redcentric personnel.

7.9 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)

8. Information Assurance

Certifications

Redcentric is 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's 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 aligned with:

- The Government 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 Government Security Classification Policy 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
- ISO 22301:2019 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

Network connectivity

- The Public Internet via Private or Public IP VPN
- The HSCN Peering Exchange
- PSTN
- PSN-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 regarding the Redcentric assurance and governance framework can be found within the Redcentric customer security pack, which consists 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.

Head Office

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522

E sayhello@redcentricplc.com

W www.redcentricplc.com

redcentric

