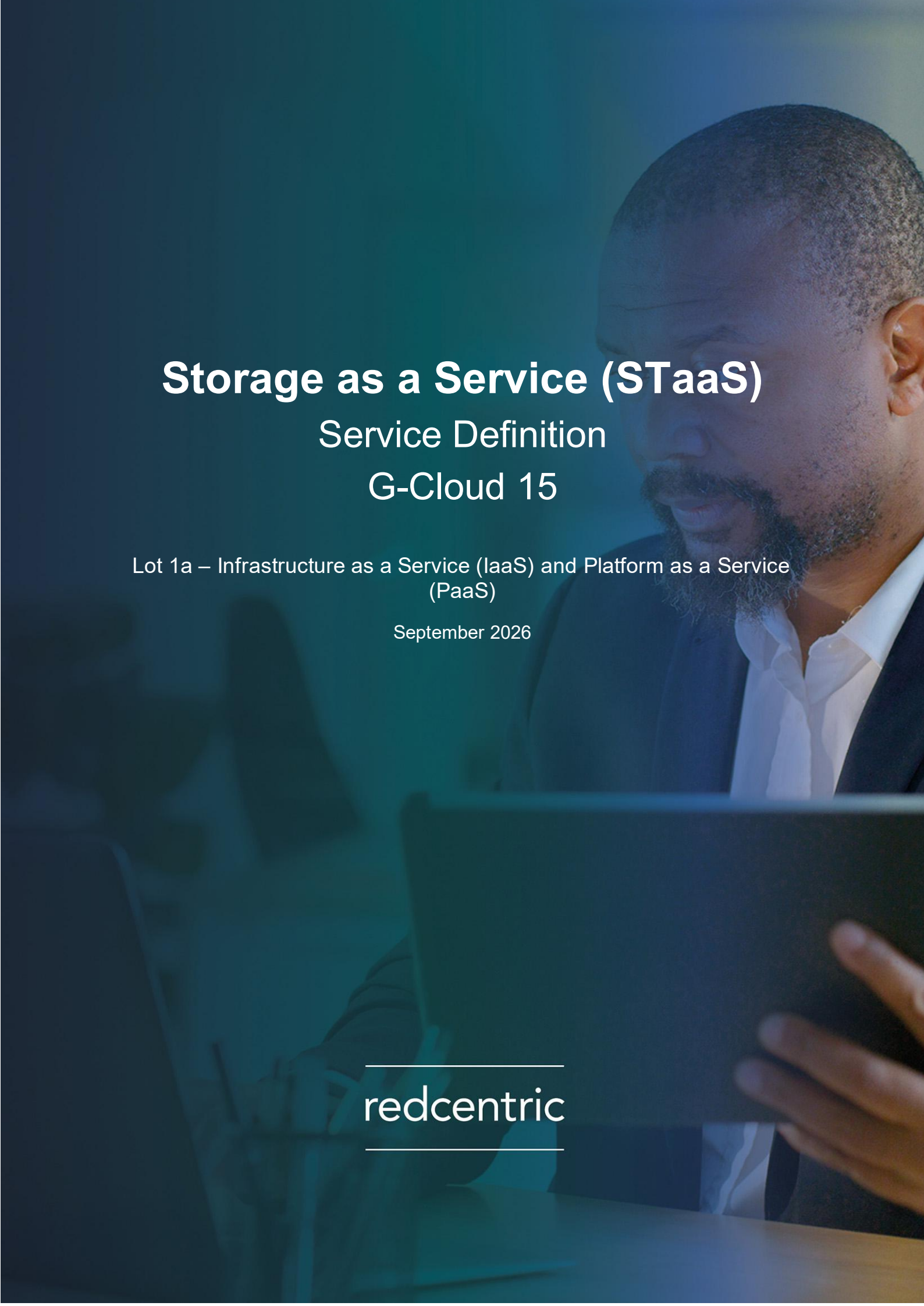




Storage as a Service (STaaS)

Service Definition

G-Cloud 15

Lot 1a – Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)

September 2026

redcentric

Contents

1.	Service Definition	3
1.1	Key Features	3
1.2	Key Benefits.....	3
1.3	Scope of Services	4
1.4	Service Requirements.....	6
2.	Onboarding and Offboarding	7
2.1	Migration Support	7
2.2	Onboarding	7
2.3	Service Delivery Management.....	8
2.4	Scope Inclusions	8
3.	Service Levels.....	10
3.1	Service Hours Definition	10
3.2	Applicable Service Hours.....	10
3.3	Service Levels	10
4.	Responsibilities	12
5.	Associated Services.....	13
6.	Business Continuity and Disaster Recovery	14
7.	Data Management.....	16
8.	Information Assurance	18

1. Service Definition

This service definition details the scope and operation of the Redcentric Storage as a Service (STaaS) product. The product is offered across two tiers which provide storage management, infrastructure, and provisioning.

The Redcentric STaaS is an ITIL aligned standard, repeatable storage infrastructure, provisioning, and management service.

1.1 Key Features

STaaS provides cost-effective, resilient storage capacity backed by market-leading vendors including NetApp and HPE, hosted in our partner UK data centres.

Costs are charged on a per GB basis which includes storage management, infrastructure, licensing, and networking. The product is delivered in a repeatable manner using standard processes, tools, and automation. The following service definition provides a detailed definition of service features and associated SLAs. It also describes out of scope activities and linked complementary Redcentric services.

The following illustrates the benefits of partnering with Redcentric:

- Capacity scaling
- Tier 3 data centres
- Monitoring and observability
- Encryption
- Patching
- Access to the Redcentric network
- High availability

1.2 Key Benefits

- Reduced storage TCO through improved utilisation, enabling customers to continually right-size the solution based on capacity and performance needs at specific points in time
- Eliminates need for Capex investment
- Reduced licence management and simplified procurement
- Reduced support costs
- Reduced cyber threat exposure through adoption of vendor recommended architecture and vendor cyber expertise
- Reduced cost and timescales for design/build/migration phase
- Provides customer access to advanced technical capability and vendor expertise
- Access to vendor discounts and Redcentric network reduces costs
- Reduced investment in commodity technology, enabling investment in value-added innovation such as IoT, machine learning, AI and big data
- Futureproof platform that will evolve and develop to reflect latest technologies and changing customer requirements

1.3 Scope of Services

1.3.1 Performance Tiers

Redcentric STaaS has two (2) performance tiers intended to reflect different use cases and to align a customer's business needs and budget appropriately.

Tier	Premium	Standard
Best for	Databases, virtualised applications, software development, AI/ML	File shares, web servers, log files, backup files and replication targets
Max IOPS/TiB (effective capacity)	2048	512
Max throughput MBps/TiB	64	16
Latency	< 1 ms	< 4 ms
Minimum commitment	25 TiB	50 TiB

1.3.2 Storage Platform Support

- Incident resolution using a standard Incident Management System
- Escalation and engagement with vendors as necessary
- Root cause analyses performed for P1 incidents
- Management and execution of changes in accordance with standard change management processes and tools
- Representation and participation in the incident management process

1.3.3 Capacity Scaling

- Increase in capacity within contracted tolerance within 5 business days of request being submitted
- Decrease in capacity within contracted tolerance
- Plan for and provide storage changes due to business growth and project implementation, based on information supplied by the customer, and review plans with the customer on a consistent basis
- Test and implement storage platform changes, in accordance with proper change management procedures

Changes in capacity outside the contracted capacity will be managed through a review of existing capacity needs and contract refresh. Delivery timeframes will be on a best endeavours basis.

1.3.4 Tier 3 Data Centres

- Tier 3 ISO aligned data centres
- Carrier neutral
- Minimum N+1 redundancy of power to the data centre
- Minimum N+1 redundancy on the chilled water-cooling system
- Security onsite 24/7/365
- Analogue addressable fire detection system in all areas

1.3.5 Monitoring, Observability and Reporting

- Monitor storage infrastructure integrity
- Disk capacity monitoring and alerting
- Monitor storage backups and replication
- Review of storage capacity/performance and recommendations on optimisation
- Monitor storage platform error logs
- Provision and maintenance of Database support reporting via self-service default dashboard
- Default dashboard includes capacity, IOPS and throughput.
- Requests to modify the default dashboard view will be considered and are subject to additional Professional Services charges.

1.3.6 Security & Encryption

- Implementation of, and adherence to, relevant agreed, customer IT policies and procedures and in accordance with Redcentric standard processes
- Security audit compliance in adherence to agreed customer IT policies and procedures and in accordance with Redcentric standard processes
- Security patch updates (hot fix)
- Customer Unique Encryption (Shared / Dedicated)

1.3.7 Patching

- The patch management service provides a quarterly security review and remediation process.
- Redcentric will provide suitable engineering resources to meet the agreed patching schedule
- Raising any Service request for patching

The customer is responsible for:

- Supporting the required patching schedules including maintenance windows with Redcentric.
- Redcentric shall not be liable to the customer (including, without limitation, to meet Service Levels) if the customer fails to agree to planned outage windows.

1.3.8 Access to the Redcentric Network

Redcentric STaaS offers a comprehensive solution, integrating network and SAN connectivity for enhanced flexibility and security throughout the service lifecycle. This holistic approach ensures a seamless and reliable storage solution aligned with customers' network requirements, simplifying management and improving IT infrastructure resilience and performance.

- 10Gbit Ethernet connectivity to the shared STaaS network
- 1Gbit Ethernet where required for legacy support
- 32/16 Gb Fibre Channel connectivity to the shared STaaS SAN. Additional zoning on request.
- Remote access / Site mirroring
- Customer dedicated solutions

-
- Customer owned hardware integration solutions

1.3.9 Unified storage (Block/File)

- Single storage protocol (Block)
- Single storage protocol (File)

1.4 Service Requirements

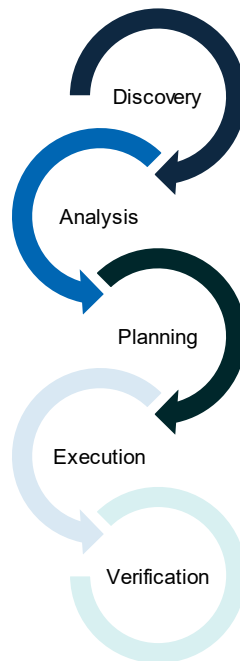
Below is a list of requirements for Redcentric to be able to deliver storage services. Some are strict requirements unless stated as optional, depending on what the customer has consumed on the STaaS platform.

Required Item	Description
Internet	Outbound internet access for reporting.
Access Documentation	Client is provided with information on support access methods.
Ticketing	All Priority 1 incidents are logged, and the client must follow up with a telephone call into support.
Customer Connectivity	External or off-site connectivity to storage resources is the responsibility of the Customer. This Service Definition does not include the supply of any connectivity Services from Redcentric. Redcentric connectivity Services can be supplied if required, subject to a separate Order.
System requirements	It is the Customer's obligation to make sure that their own systems work in conjunction with the Redcentric storage platform. Redcentric will assist with the hardware interoperability validation during the service scoping phase.

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, where supported by 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's 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 run through how the customer will be onboarded, 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 the 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, that ensures a smooth handover into project services.

The onboarding responsibilities outlined will be agreed and may vary depending on the hosting model in place, for example whether the service is Redcentric-hosted or customer-hosted.

Redcentric will appoint a project manager, either dedicated to the STaaS 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 the STaaS, as described below. Before commencement of Redcentric STaaS, the following transition tasks must be completed:

Responsibilities	
Redcentric	Customer
- Implement the Redcentric standard services toolset (e.g. monitoring). - Compile support documentation. - Align a Redcentric Storage 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 storage team should have SA access.	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.

2.4 Scope Inclusions

In the event of a hierarchical service escalation, work with the service desk and operations team to ensure the BAU service is restored.

Own any deficiencies in service and act on new requirements that would modify the contract.

At regular intervals, measure customer satisfaction with Redcentric services and use trends over time 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 on-site 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 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 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 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 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.

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 and the Redcentric 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.

Service Availability target is defined as the percentage of time for which the service is available to the users.

Service Availability = $\frac{\text{Agreed Service Hours} - \text{Service Downtime Hours}}{\text{Agreed Service Hours}} \times 100$

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

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

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

Testing

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

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

Network Resilience

Our network 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.

6.2 Disaster Recovery

Resilience is built into the STaaS platform. The use of NetApp ONTAP software supports three levels of RAID protection for local tiers (aggregates). The level of RAID protection determines the number of parity disks available for data recovery in the event of disk failures. With RAID protection, if there is a data disk failure in a RAID group, ONTAP can replace the failed disk with a spare disk and use parity data to reconstruct the data from the failed disk.

Customers can enable additional DR capability using multi-site/multi-region architectures through active/active or active/passive configuration. This will be agreed with the customer during the design and onboarding phase.

Customers with existing NetApp storage hardware can utilise STaaS as a DR target.

Replication and SnapLock features are available within the platform as native features, meaning DR can be enabled easily.

STaaS is also compatible with Redcentric Disaster Recovery as a Service for customers that require managed DR.

7. Data Management

7.1 Personal Data Processing Statement

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

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 and provide Service, and to 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

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 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.

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, job title).
- Customer commercial and finance details (first and last names, email address, 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 adherence to ITSM (IT Service Management) best practice. ITIL (Information Technology Infrastructure Library) provides guidance 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 HSCNCNSP (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 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

