Redcentric Sovereign Cloud

Service Definition

G Cloud 15

Lot 1a - Infrastructure as a Service (IaaS) & Platform as a Service (PaaS)

January 2026

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1. Service Overview

Redcentric Sovereign Cloud for Official is a virtual private community cloud offering specifically designed and available only for use by UK Public Sector organisations, or providers delivering services to the UK Public Sector to process data marked as Official (including Official-Sensitive). Compliant PSN connectivity to the service is offered over the Public Services Network (PSN) WAN, Law Enforcement Community Network (LECN), and the Internet for consumption of the services offered. Redcentric assigns each customer with one or more Virtual Data Centre(s) (workload) comprising of the requisite compute, network and storage resources in resource pool(s) separate from other tenants.

1.1 Service Description

Redcentric offers Sovereign Cloud Services for Official in two flavours: Infrastructure as a Service (IAAS) and Platform as a Service (PAAS). For PAAS, Redcentric also offers support beyond the Operating System (OS) to include Microsoft Runtime Applications such as AD, IIS, and SQL.

Each service is available in two security domains: (1) Assured Zone and (2) Protected Zone and the security domains can optionally be securely connected through connection gateways to provide physical and logical zoning of customers' application stack. In addition, upon request, Redcentric can also connect to PSN for Policing and Enhanced Regime.

To best illustrate and provide an overview of the services, the summary table below describes the differences:

Features	IAAS Assured	IAAS Protected	PAAS Assured	PAAS Protected
Internet connected workloads	Yes	No	Yes	No
PSN Assured connected workloads	Yes	No	Yes	No
PSN Protected connected workloads	No	Yes	No	Yes
Connection gateways	Yes	Yes	Yes	Yes
PSNP Protected	No	Yes	No	Yes
PSNP Assured	No	Yes	No	Yes

The PSN Assured and Protected zones support workloads deployed to these zones. The Internet zone supports workloads deployed to this zone. Workloads cannot be connected to more than one of the aforementioned zones at any one time however, connectivity between the zones can be offered via Connection Gateways except for Protected zone to the Internet Zone directly.

The Public Services Network in Policing Protected (PSNP Protected) is a Closed User Group (CUG) operated by Vodafone over the PSN-A, using cryptographic overlays, connecting all UK police forces. PSNP Protect has a set of controls over and above PSN-A. It is generally used to exchange data between law enforcement organisations.

The Public Services Network in Policing Assured (PSNP Assured) is a Closed User Group (CUG) operated by Vodafone over the PSN-A connecting all UK police forces. PSNP Assured has a set of controls over and above PSN-A. It is generally used to exchange data between law enforcement organisations.

The Law Enforcement Community Network is a Closed User Group (CUG) overlaying the PSN connecting all UK police forces.

Within the workloads, individual server instances are defined to run the operating system and application(s). These instances are on a Redcentric dedicated, geographical and locally resilient UK Public Sector dedicated cloud infrastructure. Protection and separation between customers is enforced through virtualisation and the configuration of firewalls and other security management systems.

Redcentric Security Cleared personnel manage the service using ISO 27001 assured processes and procedures from within our UK service operations centre.

1.2 Key Features

Key Features include:

- Hosted within Redcentric operated UK data centres.
- Fully redundant multi-tenancy multi-site enterprise infrastructure.
- Supported by a dedicated Security Cleared UK-based service operations team.
- Diverse connectivity to the PSN Assured and Protected WAN, and Internet connectivity services at both sites.
- PSNP Protected (on application).
- PSNP Assured (on application).
- LECN (on application).
- Reserved Public Services Network (PSN) bandwidth.
- Up to 99.99% Availability Service Level Agreement (SLA).
- Security Domain connection gateway.
- A range of virtual machine sizes.
- Managed Operating Systems.
- Managed Runtime Applications e.g. AD, IIS, and SQL (for PaaS only).
- Dedicated physical server options (for PaaS only).
- Flexible pricing options.
- Reduced Total Cost of Ownership and minimum commitments.

1.3 User cases

Example use cases Public Sector organisations or service providers seeking to offer application services to public sector organisations:

- Requiring hosted environments for data classified as "**Official**" including "**Official-Sensitive**" throughout the application lifecycle.
- Requiring responsive deployments that provide scalable builds, release templates and cloning of environments.
- That require a fully Managed Service.
- Seeking to reduce their overall costs and compliance risks.
- Already using a UK government cloud service and looking to mitigate risks by diversifying and avoiding single supplier lock-in.
- Individual departments who use hosted applications that have peaks in computing demands and need a level of flexibility.
- Looking to consume and pay for their infrastructure within an OPEX-based financial model and seeking greater efficiency and scalability to meet the growing needs of Public Sector departments.

1.4 Service Features and Options

A summary of service features and options.

Service	Dev & Test (Alpha/Beta)	Standard (Live)	High Availability (Live)	Managed Physical Host Single Server	Managed Physical Host Cold Standby	Managed Physical Host Warm Standby
Availability SLA	99.5%	99.95%	99.99%	N/A	99.5%	99.5%
Site Failover	Optional	Optional	Yes	N/A	Optional	Optional
4hr Recovery Time Objectives	No	No	Yes	N/A	Yes	Yes
RPO down to 1 hour	Yes	Yes	Yes	N/A	Yes	Yes
VM Performance - CPU	Contended	Contended	Contended	N/A	N/A	N/A
VM Performance - RAM	Contended	Uncontended	Uncontended	N/A	N/A	N/A
Secondary Site Compute Resource Reservation	No	No	Yes	N/A	N/A	N/A
Storage Included (Tier 2)	80GB	80GB	80GB	80GB	80GB	80GB
Additional Storage Tier 0, 2, 3	Optional	Optional	Optional	Optional	Optional	Optional
Storage Snapshot	Yes	Yes	Yes	Yes	Yes	Yes
Storage Replication	Optional	Optional	Yes	N/A	Optional	Optional
Managed Firewall	Yes	Yes	Yes	Yes	Yes	Yes
Managed Load Balancing & PSN Traffic Management	Optional	Optional	Optional	Optional	Optional	Optional
Managed Operating Systems	Yes	Yes	Yes	Yes	Yes	Yes
Managed MS Runtime Apps (AD, IIS, SQL)	Yes	Yes	Yes	Yes	Yes	Yes
Platform Protective Monitoring & HIDS	Yes	Yes	Yes	Yes	Yes	Yes
Customer Asset Protective Monitoring & HIDS	Optional	Optional	Optional	Optional	Optional	Optional
PSN 'Assured' Connectivity	Yes	Yes	Yes	Yes	Yes	Yes
PSN 'Protected' Connectivity (Protected Zone only)	Yes	Yes	Yes	Yes	Yes	Yes
PSNP Protected	Yes	Yes	Yes	Yes	Yes	Yes
PSNP Assured	Yes	Yes	Yes	Yes	Yes	Yes
Reserved PSN bandwidth	Yes	Yes	Yes	Yes	Yes	Yes
Internet Connectivity (Assured Zone Only)	Yes	Yes	Yes	Yes	Yes	Yes
Security Domain Connection Gateway	Optional	Optional	Optional	Optional	Optional	Optional
Typical Use	Development App Server	Active Directory Server	Clustered Production App			

Note: Redcentric offers Customer Asset Protective Monitoring and Host Based IDS as an optional service; however, for those who choose not to take this service from Redcentric, the customer must provide adequate Protective Monitoring themselves or via a third party to meet the requirements for HMG ICT systems. Failure to do so could result in the suspension of one or more services.

1.5 Computer Services

1.5.1 Virtual Machine Sizes

Redcentric offers a range of virtual machine sizes on the shared platform. You may select from the following range of predefined virtual machines (VM).

VM Instance (Size)	vCPU	Memory (GB)	Storage (GB)
1v CPU-2GB	1	2	80
2vCPU-4GB	2	4	80
2vCPU-8GB	2	8	80
2vCPU-16GB	2	16	80
4vCPU-8GB	4	8	80
4vCPU-16GB	4	16	80
4vCPU-32GB	4	32	80
4cVCPU-64GB	4	64	80
8vCPU-16GB	8	16	80
8vCPU-32GB	8	32	80
8vCPU-48GB	8	48	80
8vCPU-64GB	8	64	80
8vCPU-96GB	8	96	80
16vCPU-16GB	16	16	80
16vCPU-32GB	16	32	80
16vCPU-48GB	16	48	80
16vCPU-64GB	16	64	80
16vCPU-96GB	16	96	80

Your VMs can be provisioned within one or more workload(s) and up to five vLAN's per VDC.

1.5.2 Virtual Machine Resource Type

Contention refers to how committed a particular resource is, typically if the Virtual RAM or Virtual CPU is oversubscribed. In non-production workloads, oversubscription can be a suitable compromise between performance and cost.

Redcentric offers three virtual machine types on the shared platform:

Dev and Test (Alpha/ Beta)

virtual machines are provisioned in contended for both CPU and RAM mode, this mode uses unreserved resources for all virtual machines, which at peak times, may result in reduced performance levels of the virtual machine workload.

Standard (Live)

virtual machines are provisioned in uncontended mode for RAM and contended mode for vCPU; this mode ensures that the RAM resources for each VM are always available to each VM.

High Availability (Live)

virtual machines are provisioned in uncontended mode for RAM and contended mode for vCPU, additionally the compute resources are reserved at the secondary site, though the VM is only active at the primary site in normal operation.

1.5.3 Virtual Machine Availability

All virtual machines operate with high availability built in at a single site to provide 99.5% availability for Dev/ Test (Alpha/ Beta) machines and 99.95% availability for Standard (Live) virtual machines.

For High Availability (Live) virtual machines, as well as single site virtual machines with optional replicated storage, all data is replicated to the second site to support an additional level of availability to provide a 99.99% SLA. Replication frequencies are based on the RPO you choose as part of your Storage Services. These typically vary from 1 hour to 12 hours.

1.5.4 Virtual Machine Cloning

Virtual Machine cloning creates a duplicate of a virtual machine with the same configuration and installed software as the original virtual machine. Virtual machine clones are additional virtual machines and are charged for accordingly based on storage and, if powered on, then Virtual Machine charges will apply.

Cloning can be undertaken on any Virtual Machine as an optional service; cloning is available via a service request and is a chargeable service request catalogue item. Charges are aligned to our published GDaD rate card as detailed in the Secure Intelligent Hands section of this Service Definition.

1.6 Customer Portal

The customer portal is available to customers includes the following features:

- Service Request Catalogue.
- Raise and Track Incidents and Service Requests.
- Charts.
- Knowledge Base.

1.7 Customer Service

Customer service requests can be raised by calling the service desk, via email (for CJSM users) or via the Service Request catalogue within the customer portal. The service desk will categorise and prioritise each service request received with the classifications in Table below:

Priority	Impact	Type
1	Critical	Change required to maintain total service operability
2	High	Change required to maintain a main element of the service
3	Medium	Change required to improve an element of the service
4	Low	Cosmetic change to an element of the service

Redcentric will acknowledge customer service requests in accordance with the timescales specified in table below.

Type	Priority	Target Time to Acknowledge Service Requests	Measure
KPI	1	15 minutes	Once the service request is categorised, classified, and assigned an owner
KPI	2	30 minutes	
KPI	3	1 hour	
KPI	4	12 hours	

Resolution times for customer service requests, including any requirements to perform work outside of normal business hours will be mutually agreed on a case-by-case basis. We will notify you if the customer service request incurs additional charges or require a change to any of your services. We will not proceed with the request until we have received your agreement to any additional costs or charges.

Table below defines the standard service requests we offer in our Service Request catalogue and indicates which service requests are chargeable. Standard Service Request pricing can be found in the Redcentric Sovereign Cloud Price Card.

Customer Service Request Type	Chargeable Service	Additional Monthly Charges
Change Firewall Rule Set (Max 5 Rules per request)	Yes	No
Change Standard Load Balancing Rule Set (Max 5 Rules per request)	Yes	No
Change Virtual Machine Resources (CPU, RAM, Storage)	No	Yes (Storage and/or compute)
Change Storage Snapshot/Replication Frequency/Retention	Yes	No
Clone Machine/Data store/VDC	Yes	Yes (Storage and/or compute)
Delete a Virtual Machine(s)	No	No
File/data upload to existing Virtual Machine/Host	No	No
Order a new Virtual Machine/Host	Yes	Yes (Storage and/or compute)
Power off a Virtual Machine/Host	No	No
Power on a Virtual Machine/Host	No	No
Rebuild Virtual Machine/Host as Initial Build	Yes	No
Restart a Virtual Machine/Host	No	No
Restore Data to a Machine from a Snapshot	Yes	No
Restore Machine from a Snapshot	Yes	No
Shutdown a VM/Host	No	No

Fair use policy will apply and service requests (those with inclusive service requests) that exceed this will be chargeable as above. Inclusive service requests do not roll over to the next calendar month.

2. Service Options

2.1 Connectivity Gateway

This optional service provides a technical architecture that will allow secure connectivity between zones, typically for those Workloads connected to two or more zones, for example workload's running in an Internet 'Assured' zone that needs to communicate with a workload in a PSN 'Assured' zone.

During the discovery and design phase, our solution and security architects, from our professional services team, will discuss your requirements and agree the controls (people, process, and technologies) required to meet the additional accreditation requirements of this service. Professional services charges will apply for this optional service.

2.2 Managed Load Balancing

A Managed Load Balancing service is optional.

This service provides single or multiple load balancing instance(s) that will load balance traffic to virtual machines and/ or Managed Physical Hosts in a single site with basic load balancing rule sets e.g. round robin, percentage traffic share and least connection.

The standard service includes up to five rule set changes per month, via service request, with a maximum of 5 rules per request. Additional rule set change requests can be made and will be charged at then current rates.

2.3 Public Services Network (PSN) Traffic Management

PSN Traffic Management allows the distribution of inbound IP traffic across our two sites. PSN traffic management is only available for customers who connect to the platform with the following PSN connectivity services:

- One or more shared user group PSN connections:
- PSN Registered DNS Zone(s);
- 1 PSN IP Address block per site per PSN 'Assured' connection

2.4 Managed Firewall Service

Managed Firewall Service consists of a virtual firewall instance and the initial context(s) configuration as standard. Also, included in the Managed Firewall Service are up to five rule set changes per month per context, via service request, with a maximum of five rules per request. Additional rule set change requests can be made and will be charged. For further detail, see the Redcentric G-Cloud Managed Firewall Service, Service Definition and Price Card.

2.5 Managed Vulnerability Scanning

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

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

- Run a scan against all customer VMs and virtual devices in scope.
- In the event of multiple subnets, the scan will be run against each one of them separately.
- Report generation.
- Report review and consolidation.

- Categorisation of risks as Critical, High, Medium, Low.
- Raise incidents records against each vulnerability for mitigation actions.
- Execute mitigation activities.

For further detail, see the Redcentric G-Cloud Managed Vulnerability Scanning, Service Definition and Price Card.

2.6 Managed Detection Response

Redcentric and its key service partners (collectively "**the Supplier**") provides a Managed Detection and Response (MDR) service, with 24/7/365 cyber security threat detection and response - see section 14 of this document for details.

The service captures and alerts on events commensurate to the data processing requirements of each environment, as stipulated by the PSN Code of Connection and the recommendations laid out in the National Cyber Security Centre (NCSC) Good Practice Guide (GPG) 13 - Protective Monitoring for ICT Systems and the CESG Architectural Pattern (AP) 1 - Audit & Monitoring across Security Domains.

2.7 Accreditation & Migration Services

2.7.1 Accreditation Advisory Services

Our Accreditation Advisory Services are available as an optional service to assist the data owner in achieving the appropriate accreditation for connectivity and compliance for consuming and publishing services from the Redcentric Sovereign Cloud Service for UK Government platform. Our consultants and advisors will formulate work packages within one or more fixed price statement of works to deliver the requirements.

One or more of the following activities will be included in the scope of the work package.

Data Gathering: This task ensures that there is a good understanding of the service being delivered to the end-customer, in particular:

- The scope of the service including the elements provided by Redcentric, the elements provided by the customer/vendor and the elements provided by the vendor's customers (i.e. Redcentric' responsibilities, customer/vendor responsibilities, the end-customer responsibilities and ownership of information assets).
- Identification and valuation of information assets within the service.
- Understanding how the service is provisioned, how the end-customer accesses the service, and how customer/vendor provides service management.
- Agreeing with the end-customer the risk appetite and risk tolerance associated with the service.

Threat Assessment: This would build upon the threat assessment of the Sovereign Cloud Services for UK Government platform and hence would only focus on the additional threats (if any) posed by the customer service being delivered to a particular end-customer.

Risk Assessment: This would build upon the Sovereign Cloud Service for UK Government platform risk assessment, focusing on the additional risks posed by the customer service being delivered to a specific customer. This will include:

- Producing an Infosec model as defined in HMG IS1 & 2.
- Identify potential compromise methods and their associated risks.
- Produce a prioritised list of risks based upon the capability and motivation of specific threat actors and the potential impact of a particular compromise.

Risk Treatment Plan: Using the above risk assessment and building upon the Sovereign Cloud Services for UK Government risk treatment plan, this task will identify the degree of compliance with the security controls specified in HMG IS1 & 2. This will include identifying how assurance in those controls is achieved.

Residual Risk Assessment: This task will identify any risks that are not adequately treated by the Risk Treatment Plan and produce a remediation plan for resolving those risks.

RMADS Production: This task will collate the results of all the previous tasks and produce a Risk Management and Accreditation Document Set (RMADS) in accordance with HMG IS1 & 2. This process will involve drafting, reviewing, and updating activities with the end-customer accreditor. The outcome of this task will be approval from the end-customer accreditor and Senior Risk Owner that the customer service for that customer can operate at the required security level.

2.7.2 IT Health Check Service

Working with CESG approved partners, Redcentric offers, as an optional service, an IT Health Check (penetration test) service under the CHECK scheme to identify vulnerabilities in the IT systems that you plan to run on the Sovereign Cloud Services for UK Government environment.

The IT Health Check is a necessary part of the data owner's (SIRO) responsibilities to ensure the correct implementation of security functionality and to identify and mitigate vulnerabilities in the application workloads, which may otherwise compromise confidentiality, integrity, or availability of information on the system or network. All systems processing data protectively marked Official, including Official-Sensitive, must be assessed under CHECK.

2.7.3 Approach of the IT Health Check Service

Each assessment performed under the terms and conditions of CHECK will be performed by a team of security cleared (SC) personnel and led by a CHECK team leader. He or she will be present throughout the test.

A CHECK assessment is an IT Security Health CHECK conducted in accordance with procedures and standards laid down by CESG.

There is no fixed technical specification for a CHECK assessment, so, in the first instance, such an assignment must be properly scoped by an accredited CHECK Team Leader. On acceptance of the scope of work, testing will be conducted by a CHECK Team, consisting of at least one qualified CHECK team leader and several CHECK team members.

2.7.4 IT Health Check Report

Our Accreditation.

Our CESG approved IT Health Check partner will provide a penetration testing report with a full understanding of any vulnerabilities within an environment on the Sovereign Cloud Services for UK Government platform, as well as specific advice on how to eliminate or mitigate those vulnerabilities.

At a high level the report will include the following information:

- A non-technical summary of the Health Check findings.
- An objective or aim for the Health Check.
- The Scope of the Health Check is agreed with the customer.
- The vulnerability findings.
- Recommendations/ solutions.
- Basic logs.

More specifically, the following items will be included in the report:

- Individuals involved in the test are identified.
- A high-level description of the main findings in non-technical terms.
- All findings are positively identified (where possible) and described.
- Each finding is accompanied by a solution that is relevant to the customer's environment.
- Automated vulnerability scanning tools do not appear to have been heavily relied upon.
- The tests and attacks performed were as comprehensive as possible, technically sound and within the bounds of the customer agreed scope.
- The logs should contain full port scans for each live system within scope and show how each live system was identified.

2.8 Migration Services

Redcentric also offers a chargeable full migration service. The migration service provides a low risk, benefit optimised transition plan to migrate your services onto the platform. Using proven methodology, tools and experience gained from prior migrations, the service consists of a highly collaborative process that works closely with your IT and business teams.

This approach enables Redcentric to develop and execute a migration plan based on proven strategies that incorporate validation of workload compatibility, dependencies, rollback plans and testing of candidate services including an evaluation of application performance pre and post migration.

2.9 Transitional Hosting

Redcentric can offer a transitional hosting option to de-risk cloud migration in the circumstance of a compelling event with a hard deadline. Transitional Hosting is an interim only solution for use whilst design of the target estate and migration is completed. This transitional option is only available as an element of a full cloud migration.

3. Management Services

3.1 PSN Assured and PSN Protected

The platform has dual site dual path connectivity to the Public Services Network (PSN) Assured and Protected WAN. The platform service interfaces to the PSN are via dedicated customer virtual firewalls and optional traffic management/ load balancing services per customer workload.

Customers and user communities will require access to the PSN and must comply with the PSN Code of Connection (CoCo) to access the services hosted on the Managed Cloud Services for UK Government platform. Redcentric supports access via the PSN shared user groups.

Customers must reserve the bandwidth for each PSN connected workload. This is available in 1Mbps increments, charges apply. Customers must obtain their own IP Address Blocks for PSN use from the Cabinet Office.

3.2 PSNP Protected and PSNP Assured

The Public Services Network in Policing Protected (PSNP Protected) is a Closed User Group (CUG) operated by Vodafone over the PSN-A, using cryptographic overlays, connecting all UK police forces. PSNP (Protect) is a set of controls over and above PSN-A. It is generally used to exchange data between law enforcement organisations.

There are 20Mbps and 100Mbps encryption devices available with usable bandwidth of 80% of the stated throughput. Each encryption device can only have one IP address and dedicated per customer environment. If a high availability pair is required in one site for resiliency, then 2 encryption devices will be needed.

The Public Services Network in Policing Assured (PSNP Assured) is a Closed User Group (CUG) operated by Vodafone over the PSN-A connecting all UK police forces. PSNP Assured has a set of controls over and above PSN-A. It is generally used to exchange data between law enforcement organisations.

Redcentric is an approved third-party supplier to connect to these networks having satisfied the NPIRMT information assurance requirements. The connection to Redcentric Government Cloud Protected Zone is a private circuit provided and managed by Vodafone.

When connecting to a PSNP Protected and/or PSNP Assured you will need to wait for Vodafone to provision the connectivity into the Redcentric' datacentres. Because of this you will need to factor in an extended lead time.

When connecting to the PSNP Protected and/or PSNP Assured you will need to obtain the required IP addresses directly from the Home Office and have them assigned to your solution to be hosted by Redcentric.

3.3 PSN Assured and PSN Protected

Redcentric can provide secure remote access laptop(s), as an optional chargeable service to support non-PSN secure access to the platform for Third Parties e.g. Independent Software Vendors, who publish applications for PSN connected customers. Remote access laptops are available for a minimum period of 12 months.

Limitations of Use

- All Administrators that access the device must have validated SC clearance.
- The supplied device can only be used to connect to the platform.
- Up to 3 named users per device.

What is Included

- Laptop and power supply.
- RSA Hard token(s) 3 maximum.

Provisioning and Support Process

The remote access laptops are built and supported by Redcentric secure operations team. Each device is individual and registered to its users.

Users will need to enrol to the whole disk encryption service with their token and credentials. All registered user(s) for each device will need to produce their Systems Operations Procedures (SYOPS) and sign our (SYOPS) before they can be issued with a remote access laptop.

If the user requires support for the device, or if the device fails, you should contact the Redcentric Managed Cloud Services for UK Government service desk. Redcentric will arrange for the faulty device to be returned to the service desk team for replacement. On receipt of the faulty device, Redcentric will dispatch a new device for next business day delivery.

In the event of loss or theft of a remote access device, the partner or customer must inform the Redcentric secure operations team immediately.

Devices remain the property of Redcentric and must be returned at the end of the contract/ life. Laptops will be replaced every 3 years.

3.4 Virtual Desktop for Administrator Remote Access

In addition to the provision of remote laptops, Redcentric can provision remote access via secure virtual desktops, based on AWS Workspaces. This is an optional chargeable service to support non-PSN secure access. AWS Workspaces are subject to maintenance windows that may interrupt access and Redcentric strongly recommend that at least 2 Secure Laptops are subscribed to mitigate the potential for AWS Maintenance windows to interrupt access.

Limitations of Use

All Administrators that are provided with access to the Redcentric management network via the Virtual Desktop must have validated SC clearance.

The Virtual Device can only be used to connect to the management network.

What is Included

- Access to appropriately spec'd AWS Workspace.
- Access to multi-factor authentication

Provisioning and Support Process

Authorised users are provided with access to a virtual desktop by Redcentric secure operations team. Each virtual desktop is individual and registered to a single users. The user will need to produce their Systems Operations Procedures (SYOPS) and sign our (SYOPS) before they can be issued with access to a virtual desktop.

Physical Laptop users will need to enrol to the whole disk encryption service with their token and credentials. All registered user(s) for each device will need to produce their Systems Operations Procedures (SYOPS) and sign our (SYOPS) before they can be issued with a remote access laptop.

If the user requires support, you should contact the Redcentric Managed Cloud Services for UK Government service desk.

In the event of loss or theft of a multi factor authentication device, the partner or customer must inform the Redcentric secure operations team immediately.

3.5 Managed Internet Access

Redcentric Access as a Service provides highly available IP access to the Internet. It not available on the Protected Zone. For more detail, please refer to the Redcentric G-Cloud Access as a Service, Service Definition and Price Card.

3.6 Inter-Site Connectivity

Customers can deploy virtual machines on the shared platform and Managed Physical Hosts across both sites to give higher levels of application availability. For dual site design services, you will need to order inter-site connectivity with the appropriate amount of bandwidth reserved across the inter-site link. Bandwidth is available in 1Mbps increments, charges apply.

3.7 Secure Intelligent Hands

The secure intelligent hands service provides the facility for Redcentric to assist with the provisioning of customer services on or off from the Sovereign Cloud Services for UK Government platform using Redcentric personnel who have been granted Security Clearance.

When physical access or remote access is required into the secure sites where Redcentric operate the Sovereign Cloud Services for UK Government platform services, Redcentric will provide the necessary skilled Security Cleared personnel, adhering to our mandated security controls, to complete the necessary tasks.

One example task where the use of Redcentric secure intelligent hands would be required would be for the direct import or export of customer data into or out of the platform as only Redcentric security cleared staff may enter the restricted sites where the platform is located.

Another example would be where Redcentric would facilitate remote access to the platform via a secure remote access laptop where the customer's designated operator of the laptop did not have validated Security Clearance in place (a mandatory requirement for remote access) at the time, but access to the environment was required to carry out some critical work. Redcentric secure intelligent hands can chaperone the customer whilst the work is undertaken.

Customers can order secure intelligent hands via a G-Cloud contract with the number of half days to be utilised throughout the period of the contract. The minimum secure intelligent hands order is for half a day per site either in normal business hours 8:00am to 6:00pm (UK time, Mon to Fri excluding UK Bank Holidays) or Out-of-Business Hours (All other times). Additional charges will apply as specified in the Redcentric Sovereign Cloud Price Card and Cloud Services SFIA rate card.

Secure Intelligent Hands type	Professional Service Charge
Business Hours (Monday to Friday 8am to 6pm)	Half Day
Out-of-Business Hours (Monday to Friday, Weekends, UK Bank Holidays)	Half Day

All Secure Intelligent Hands requests must be made by raising a service request via email or the customer portal. Redcentric will provide reasonable endeavours to schedule the Secure Intelligent Hands resource within 5 business days of the Secure Intelligent Hands service request being categorised, classified, and assigned an owner.

3.8 Secure Direct Data Import and Export Service

The Redcentric Secure Direct Data Import and Export Service allow customers of the Sovereign Cloud Services for UK Government platform to transfer their data into and out of their VDCs via a Secure Data Transfer Server at each site. Typically, this would be for larger data files, database files or potentially application installation ISO images.

The Secure Direct Data Transfer Service allows for the connection of a portable USB device to the Data Transfer server within the platform and supports the controlled, (virus and malware checking and quarantining) import and export of data to and from customer data stores.

The service is designed to enable the customer to maintain full control over the access to their data through every stage of the process in accordance with their specific data handling procedures.

4. Managed Operating Systems

4.1 Shared Platform Virtual Machines

Redcentric will deploy, monitor, and manage the supported operating system(s) as well as deploying agents to monitor the platform's continued health. Redcentric will maintain the patch state of the operating system, deploy anti-virus/malware software, and monitor uptime and performance. Redcentric is not responsible for the management of additional Windows Server Services, for example DHCP Servers, Certificate Services that the customer may introduce on to the server. This also applies to Linux operating systems. Please refer to section 9 "Managed Operating System Services" for more detailed information.

Redcentric provides all operating system licences for use on this platform. We may also need to provide other software licences; Redcentric will work with you to understand the overall licencing requirements for each customer solution.

4.2 Microsoft Runtime Application Services

Redcentric provides the following supported Microsoft Runtime Application Services in addition to supporting the operating systems mentioned above:

- Microsoft Active Directory
- Microsoft SQL Server
- Microsoft IIS
- Microsoft Exchange Server

The scope for the design, build, and service take-on for Microsoft Runtime Applications Services will be agreed between Redcentric and the customer and will be formulated into work packages within one or more fixed price statement of works to deliver the requirements. Please refer to section 10 "Microsoft Runtime Application Services" for more detailed information

4.3 Reverse Proxy Services

Redcentric provides support for the following reverse proxy solutions in addition to supporting the operating systems mentioned above:

- Squid Proxy

The scope for the design, build, and service take-on for Reverse Proxy Services will be agreed between Redcentric and the customer and will be formulated into work packages within one or more fixed price statement of works to deliver the requirements. Please refer to section 11 "Managed Reverse Proxy Services" for more detailed information

4.4 Storage Services

Redcentric offers Sovereign Each customer is allocated one or more data store(s) which can be provisioned from the following storage performance tiers:

- **Tier 0+ Standard Storage** - NVMe Solid-State Drives (SSD) with a target performance of 4000 IOPS per terabyte with a single off site daily recovery point (this is overwritten every 24 hours)
- **Tier 0+ Replicated Storage** – NVMe Solid-State Drives (SSD) with a target performance of 4000 IOPS per terabyte, asynchronously replicated to the second site. Multiple recovery points can be provided in both data centres as defined in section 4.5
- **Tier 0 Standard Storage** - entirely comprised of Solid-State Drives (SSD) with a target performance of 2000 IOPS per terabyte with a single off site daily recovery point (this is overwritten every 24 hours)

- **Tier 0 Replicated Storage** – entirely comprised of Solid-State Drives (SSD) with a target performance of 2000 IOPS per terabyte, asynchronously replicated to the second site. Multiple recovery points can be provided in both data centres as defined in section 4.5
- **Tier 2 Standard Storage** – comprised of Serial Attached SCSI (SAS) Hard Disk Drives with a target performance of 250 IOPS per terabyte with a single off site daily recovery point (this is overwritten every 24 hours)
- **Tier 2 Replicated Storage** – comprised of Serial Attached SCSI (SAS) Hard Disk Drives with a target performance of 250 IOPS per terabyte, asynchronously replicated to the second site. Multiple recovery points can be provided in both data centres as defined in section 4.5
- **Tier 3 Standard Storage** – comprised of Serial ATA (SATA) Hard Disk Drives with a target performance of 50 IOPS per terabyte with a single off site daily recovery point (this is overwritten every 24 hours)
- **Tier 3 Replicated Storage** – comprised of Serial ATA (SATA) Hard Disk Drives with a target performance of 50 IOPS per terabyte, asynchronously replicated to the second site. Multiple recovery points can be provided in both data centres as defined in section 4.5

Data stores cannot span multiple storage tiers. One or more data stores can be provisioned for each workload. Data stores do not span multiple workloads. * Previous Tier 1 technology deprecated.

4.5 Virtual Machine and Managed Physical Host Storage

All shared platform virtual machines and Managed Physical Hosts include 80GB of storage as a single drive. Further storage can be ordered and will be provisioned to one or more of your virtual machines or Managed Physical Hosts to facilitate additional drive partitions. Storage allocated by your shared platform virtual machines and Managed Physical Hosts within each data store will be charged per GB monthly. All Virtual Machine types and Managed Physical Hosts are unable to share virtual disks.

4.6 Storage Snapshots

Redcentric will take scheduled storage snapshots for all shared platform virtual machines and Managed Physical Hosts to facilitate recovery to a point in time, down to a Recovery Point Objective (RPO) of one hour. To support the One Hour RPO Redcentric standard recommended Snapshot intervals are as follows:

- one-hour snapshots are maintained for no longer than 5 days
- daily snapshots will be maintained for a further 26 days

The snapshot parameters will be set during the design phase so that the frequency and retention times you require can be supported to match your requirements. Changes to your snapshot regime(s) can be made via a service request and will be charged accordingly, at the published rate at that time. The storage required for snapshots must be accounted for when calculating your total storage pool, considering the number of snapshots retained and the frequency of snapshots taken.

Restoration of data from a snapshot is initiated via a Service Request and is a chargeable item.

4.7 Storage Replication

Secondary site storage replication is available to support recovery of shared platform virtual machines and Dual Site Managed Physical Host deployments only.

For Dev and Test (Alpha/ Beta) and Standard (Live) virtual machines on the shared platform you can choose between non-replicated storage and replicated storage. If you choose replicated storage for these virtual machine types, Redcentric will provide an RPO SLA down to 1 hour at the secondary site. However, Redcentric will not provide a secondary site Recovery Time Objective (RTO) SLA, we will recover your virtual machines under reasonable endeavours.

Boot storage replication will be configured for all High Availability (Live) virtual machines per the specified frequencies. For Dual Site Managed Physical Host deployments, storage replication must be ordered for

the SAN boot devices on each Managed Physical Host on the Primary Site deployed in a Dual Site configuration. Redcentric will provide a four-hour RTO SLA for the aforementioned virtual machine and Managed Physical Host types.

Your storage replication policies (frequencies and retention) will be set during the on-boarding process, see table below for supported schedules.

Retention	1 day	7 days	14 days	21 days	31 days
Frequency	Down to every hour				

Changes to the replication policies can be made in service by raising a service request and will be charged accordingly at the published rate at that time.

5. Associated Redcentric Services

The table below provide details of other compatible services with Redcentric Sovereign Cloud available from G-Cloud 15.

Service Name	Service Summary
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.
Cyber Security Professional Services	**Cyber Security Professional Services** Redcentric offers a wide range of Cyber Security Professional Services from strategy to implementation. Aligned to the NIST Cyber Security Framework, our qualified industry professionals will support you in overcoming your cyber security challenges around governance, InfoSec compliance, security testing, vulnerability management, business continuity, disaster recovery, data breach and Incident Response.
Operating System as a Service	**Operating System as a Service** will manage servers provided on the Redcentric Cloud, hosted physical server services, or managed public cloud infrastructure Managed Public Cloud AWS and Managed Public Cloud Azure. The service provides access to our support capability, technical skills, and economies of scale, to manage the customer's server operating systems.
Retained Cyber Incident Response Service	**Retained Cyber Incident Response Service** from Redcentric Cyber Security services provides on-demand and SLA-backed access to our incident response security specialists in the event of a major cyber security incident to contain and eradicate live security threats affecting your network and business operations
Vulnerability Management Service	**Vulnerability Management Service** enables organisations to identify, prioritise, and remediate software vulnerabilities affecting their digital infrastructure, applications, and services that can be exploited by a cyber attacker to cause harm to their business. We will perform regular vulnerability scanning of your internal and external (internet-facing) assets.

6. Service Availability

6.1 Service Support

In provision of the Redcentric Sovereign Cloud Services for UK Government, Redcentric will provide to all customers of these services four key capabilities:

Service Desk – provided on a 24/7/365 basis, the Redcentric Service Desk is the central point of contact for all service-related communications with Redcentric for all subscribed services who will liaise with the customer authorised personnel to log any issues, requests or enquiries relating to these services. The Redcentric Service Desk will ensure that calls are passed to the appropriate resolver groups for follow up and resolution.

Service Operations – available on a 24/7 basis, the service operations teams will include an on-site presence at the appropriate data centres, providing additional support resources to the technical support teams tasked with ensuring that prescribed SLAs are maintained.

Service Management – a team of dedicated Service Management specialists who liaise directly with Redcentric Service Operations to ensure correct levels of governance and compliance are in place and aligned with ITIL best practice guidelines.

Systems Support and Administration – Redcentric will provide these technical support functions to the Redcentric Sovereign Cloud Services for Official platform and PaaS customers.

Further details can be found in the Redcentric Sovereign Cloud Operations Manual, which is owned by Redcentric Service Management. This Operations Manual describes the policies, processes, procedures, and interfaces through which the services are delivered.

6.2 Service Level Agreements (SLAs)

6.2.1 Service Desk and Support Windows

Redcentric Sovereign Cloud Services for Official adheres to the following service desk availability and support windows.

Server Type	Service Desk	Support Window
Dev and Test (Alpha/Beta) virtual machines on shared platform.	24/7	8:00am to 6:00pm UK time, Mon to Fri excluding UK holidays and out of hours (OOH) for change implementation and P1/P2 support when required.
Standard (Live) and High Availability (Live) virtual machines on shared platform and Managed Physical Hosts.	24/7	24/7

6.2.2 Virtual Machine

Virtual Machine availability is measured on a per virtual machine basis on the shared platform where the service comprises both the server and storage associated with it.

Sovereign Cloud Services for Official adheres to the following virtual machine availability targets.

Virtual Machine Type	System Availability Target	Definition
High Availability (Live) shared platform VM	99.99%	Either primary or secondary server is up and OS and/or Application is operational if managed by Redcentric

Virtual Machine Type	System Availability Target	Definition
Standard (Live) shared platform VM	99.95%	Availability on a per server basis and OS and/or Application is operational if managed by Redcentric.
Dev and Test (Alpha/Beta) shared platform	99.5%	Availability on a per server basis and OS and/or Application is operational if managed by Redcentric

A shared platform virtual machine is deemed available when the operating system responds to ICMP (Ping) requests.

6.2.3 Managed Physical Hosts

Managed Physical Hosts in Sovereign Cloud Services for Official offers the following availability targets.

Type	Physical Host Deployment	System Availability Target	Definition
KPI	Single Server	98.5%	Physical server is up and OS and/or Application is operational if managed by Redcentric
SLA	All other Managed Physical Host deployment types	99.5%	Either primary or standby (secondary) server is up and OS and/or Application is operational if managed by Redcentric

6.2.4 Recovery Point Objective

Sovereign Cloud Services for Official adheres to the following RPO targets.

Type	Server Type	RPO Target	Definition
SLA	All Shared Platform Virtual Machines All Managed Physical Host types	Set during on-boarding (down to every hour standard maximum) and any changes via service request in life.	Recover to last snapshot as defined by RPO target.

6.2.5 Recovery Time Objective

Sovereign Cloud Services for Official adheres to the following RPO targets. Virtual Machines and Managed Physical Hosts. Sovereign Cloud Services for Official adheres to the following RTO target for High Availability (Live) virtual machines only.

Type	Server Type	RTO Target	Definition
SLA	High Availability (Live) Virtual machines on shared platform.	4 hours	The HA virtual machine OS at the secondary site is recovered to the required running state.
SLA	All Dual Site Managed Physical Host Types	4 hours	The standby server OS in the secondary site is recovered to the required running state

6.2.6 Internet Access

Internet Access availability is defined as the ability to route a data packet from a customer's private segment to the egress point on the public Internet. Meeting this SLA is based on an Availability Percentage of 99.99% as calculated in the following table.

Variable	Definition
Monthly Hours	Total number of hours in any month.
Scheduled Downtime	Total time in the month that the service is scheduled as unavailable either by maintenance or by customer request.
Unscheduled Downtime	Total time in the month that the service was unavailable due to an action by Redcentric unrelated to scheduled downtime. Obtained from ICAP.
Scheduled Uptime	Monthly hours minus Scheduled Downtime.
Available Hours	Scheduled Uptime minus Unscheduled Downtime.
Availability Percent	Available Hours divided by Scheduled Uptime, rounded to the nearest 10th.

Outages caused by the following events are not included as Unscheduled Downtime:

- Hardware failures unrelated to Redcentric negligence or Redcentric infrastructure.
- Software failures unrelated to Redcentric negligence or Redcentric infrastructure.
- Breach of acceptable use policy or any breach of the agreement by the customer or customer agent.
- Negligence or intentional acts or omissions by the customer or customer's agent.

The Commitment becomes void if any one of the following occurs:

- The customer refuses a Redcentric maintenance change request related to the delivery of Internet Access services.

6.3 Incident Priority Definitions

The Sovereign Cloud Services for Official use the following criteria for prioritisation of incidents as defined in the Redcentric Sovereign Cloud Services for Official contract.

Priority	Contact Method	Criteria (Meets One or More)	Examples (Not a Definitive List)
P1	By Phone to meet OLA. Ticket must also be created	Severe unusable. Severe disruption of service or business functions, possibly with revenue loss. Critical Systems Unit failed or severely impaired. No workaround(s) exist. Affects Critical business unit, users, or functions.	Multiple server failures affecting key operational areas. Severe performance degradation. Financial systems affected in a close period. Security issue such as malware, virus.
P2	By Phone to meet OLA. Ticket must also be created	Causes major business disruption. VIP user(s) or Business Unit with significant reduction in system performance. No workaround(s) exist. Potential to cause or become a P1.	Slow response of key business application for one or more users. Security incident.
P3	Ticket in customer portal	Impacts system availability or operation of services. Affects users within a single function. Workarounds may be in place. Business operations impacted but not severely.	Equipment failures which are covered by redundancy/ resiliency. Server or infrastructure device identified as not having current patch/pattern files within 5 days of a patch being uploaded to the distribution servers by Service Provider.
P4	Ticket in customer portal	Minor disruption or usability issues. Affects single user or function. Workaround is available. Does not impact business operations.	Incident queries relating to Data Centre Services.

6.4 Incident Response and Resolution Targets

Incidents are responded to, resolved, and reported, according to the Key Performance Indicator (KPI) specifications as listed below.

	Type	Service Level	Target	Measure
Response Times	KPI	Priority 1 (Critical)	15 mins	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
	KPI	Priority 2 (High)	30 mins	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
	KPI	Priority 3 (Medium)	60 mins	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
	KPI	Priority 4 (Low)	2 hours	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
Resolution Times	KPI	Priority 1 (Critical)	4 hours	For each Priority 1 (Critical) Incident, from the time the Ticket is logged in the Ticket Management System, to the time that the Incident is resolved.
	KPI	Priority 2 (High)	8 hours	For each Priority 2 (High) Incident, from the time the Ticket is logged in the Ticket Management System, to the time that the Incident is resolved.
	KPI	Priority 3 (Medium)	4 business days	For each Priority 3 (Medium) Incident, from the time the Ticket is logged in the Ticket Management System, to the time that the Incident is resolved.
	KPI	Priority 4 (Low)	10 business days	For each Priority 4 (Low) Incident, from the time the Ticket is logged in the Ticket Management System, to the time that the Incident is resolved.
Updates	KPI	Priority 1 Incident	every hour (24x7)	A Redcentric service desk incident assignee will contact the customer named contact by phone every hour with an update on incident status.
	KPI	Priority 2 Incident	every 2 hours (24x7)	A Redcentric service desk incident assignee will contact the customer named contact by phone every 2 hours with an update on incident status.
	KPI	Priority 3 and 4	every 24 hours Mon to Fri	A Redcentric service desk incident assignee will email the customer named contact every 24 hours Monday to Friday with an update on incident status.
Reports	KPI	Priority 1 and 2	within 4 business days of incident resolution	The Redcentric Service Manager will formulate an incident report and present it to the customer service owner.

6.5 Maintenance Windows

Incident Maintenance windows are defined to ensure Redcentric can perform routine and scheduled maintenance of the platform to maintain availability and retain certification.

Redcentric maintains the supporting infrastructure for this platform using the following principles:

- Maintenance windows will not be included in any formulas for calculating availability of the platform.
- Maintenance window times are excluded from the Availability service level calculation i.e. total time available will exclude the maintenance window times.
- Expected downtime during maintenance windows will not be included in any Service Credit calculation.
- Organisations that have deployed 'active-active' solutions should not experience any downtime during maintenance windows if the application has been implemented correctly to cater for such events; however degraded performance may be experienced.
- Redcentric retains the right to close all systems to perform emergency maintenance if non-performance of this maintenance could result in a security risk for the platform or any organisation using the platform.
- You will be allocated one 'scheduled' maintenance window per week, which will be defined during the service on-boarding process.
- Seven (7) days' notice will be provided for routine and scheduled maintenance.
- Twenty-four (24) hours' notice will be provided for critical and security related patching, unless deemed as an Emergency to stop a major outage on the platform.
- Four (4) hours' notice will be provided for emergency patches and critical changes.
- All non-emergency patches and changes will be performed on a Redcentric Managed Test workload prior to being deployed to your environments.

The following Maintenance Descriptions apply:

Redcentric maintenance windows – this will include modifications, patching or fixes to the platform or management zones, with maintenance being performed between the hours of 8pm and midnight, on the 1st and 3rd Sunday of each month at the primary site and the 2nd and 4th Sunday each month at the secondary site. Redcentric will always strive to complete the maintenance as soon as possible within the maintenance window and will only ever use the full maintenance window when necessary. The platform and management zones run on the secondary site whilst maintenance is undertaken on the primary site and vice versa.

Maintenance activities assessed as non-disruptive will be scheduled as best suits the Redcentric maintenance of infrastructure in any given organisation's zone – this will include standard and routine maintenance, including the implementation of security and critical patching, fixes or hardware and software upgrades. Where the application can support a resilient architecture that can facilitate non-disruptive changes (for instance "Blue/Green" deployments, Redcentric will design a resilient architecture to enable patching during standard business hours.

Where applications do not support this resilience, we will agree the scheduled 'maintenance day', with maintenance being performed at a time suitable to the application, out-of-hours scheduling will be charges at the standard Redcentric rates. Redcentric will always strive to complete the maintenance as soon as possible within the maintenance window and will only ever use the full maintenance window when necessary.

Emergency maintenance – this will include the implementation of any critical security patches or configuration changes that Redcentric deem necessary to protect the integrity of the platform and any given Organisation's zone.

6.6 Service Credits

6.6.1 Virtual Machine and Managed Physical Host with Standby Server

Virtual Machine Unavailability applies where the virtual machine(s) or Managed Physical Host become unresponsive due to a fault recognised at the:

- virtual machine level (hypervisor).

- enterprise supported operating system level (see 4.1 Shared Platform Virtual Machines).
- supported Microsoft applications (see 4.2 Microsoft Runtime Application Services).
- host layer.
- storage layer.
- network layer.

And not where the fault is with:

- the customers control (application, user network).
- external connectivity providers.
- community supported operating system level.
- Incompatibility between customers provided software and the operating system or patch applied to the operating system.

If Redcentric fails to meet the Virtual Machine Availability SLA for virtual machines on the shared platform or Managed Physical Hosts, then the customer is entitled to a service credit equal to the percentage identified in tables 8.6.2 to 8.6.7 for each month in which the failure occurred.

6.6.2 Dev & Test (Alpha/Beta) Virtual Machine

Service Credit percentage % of pro-rata portion of Monthly Recurring Charge for the affected virtual machine(s).

Availability (%)	Measure	Service Credit %
≥99.3% and <99.5%	VM started on alternate node and the supported Enterprise Operating System and Microsoft Application (where applicable) is operational	10%
≥99.1% and <99.3%		20%
<99.1%		30%

6.6.3 Standard (Live) Virtual Machine

Service Credit percentage % of pro-rata portion of Monthly Recurring Charge for the affected virtual machine(s).

Availability (%)	Measure	Service Credit %
≥99.9% and <99.95%	VM started on alternate node and the supported Enterprise Operating System and Microsoft Application (where applicable) is operational.	10%
≥99.5% and <99.9%		20%
<99.5		30%

6.6.4 High Availability (Live) Virtual Machine

Service Credit percentage % of pro-rata portion of Monthly Recurring Charge for the affected virtual machine(s).

Availability (%)	Measure	Service Credit %
≥99.97% and <99.99%	VM started on alternate node at Primary Site or VM started on alternate node at Secondary Site and the supported Enterprise Operating System and Microsoft Application (where applicable) is operational.	10%
≥99.95% and <99.97%		20%
<99.95%		30%

6.6.5 Managed Physical Hosts with Standby Server(s)

Service Credit percentage % of pro-rata portion of Monthly Recurring Charge for the affected virtual machine(s).

Availability (%)	Measure	Service Credit %
≥99.93% and <99.95%	Standby Server running at Primary or Secondary Site and the supported Enterprise Operating System and Microsoft Application (where applicable) is operational.	10%
≥99.91% and <99.93%		20%
<99.9%		30%

6.6.6 Recovery Point Objective

The RPO SLA is aligned to the RPO for each shared platform virtual machine or Managed Physical Host (all types) based on the storage snapshot frequency that the customer defines for each virtual machine. Redcentric will facilitate the recovery of a virtual machine(s) or Managed Physical Host (all types) to the required point in time, if the frequency and retention period set by Redcentric, but by order of the customer, can facilitate the RPO, down to a 1-hour RPO.

If Redcentric fails to meet the customer RPO SLA, then the customer is entitled to a service credit equal to the percentage identified in table RPO Service Credits below for the month in which the failure occurred.

RPO Service Credits

Service Credit percentage % of pro-rata portion of Monthly Recurring Charges based on affected virtual machine(s) and/or Managed Physical Hosts.

RPO missed by %	Service Credit %
1% to 49%	30% of monthly recurring charges
50% to 99%	40% of monthly recurring charges
100% to 199%	60% of monthly recurring charges
200% or more	100% of monthly recurring charges

6.6.7 Recovery Time Objective

Recovery Time Objectives apply to High Availability (Live) Virtual Machines and Dual Site Managed Physical Hosts with cold or warm standby servers, The RTO target time is 4 hours. Redcentric will endeavour to meet the RTO when and if it becomes necessary to fail over to the secondary Redcentric site. This is measured from the time of Redcentric acknowledgement that a site failover is required, until the virtual machine(s) and/or Managed Physical Standby Host(s) have started at the secondary site with the Operating System operational to the required running state.

Note: the RTO to fully recover the application to a consistent state may take longer and is dependent on the application. The responsibility for application recovery resides with the customer or their chosen third-party application management provider,

If Redcentric fails to meet the RTO SLA for the aforementioned server types at the secondary site, then the customer is entitled to a service credit equal to the percentage identified in the RTO Service Credit table below for each month in which the failure occurred.

RTO Service Credit

Service Credit percentage % of pro-rata portion of Monthly Recurring Charge is based on affected HA virtual machine(s) and Dual Site Managed Physical Host(s) with cold or warm standby.

RTO missed by %	Service Credit %
1% to 49%	30% of monthly recurring charges
50% to 99%	40% of monthly recurring charges
100% to 199%	60% of monthly recurring charges
200% or more	100% of monthly recurring charges

Note: The RTO service credit agreement applies for all services for which the customer has conducted a failover services test within the previous 6 months.

6.6.8 Service Credit Payments

Redcentric will pay service credits against failure to meet Server Availability SLA's or Recovery Time and/or Recovery Point Objectives but not both Server Availability SLA failures and RTO/RPO SLA failures in the same month.

Where both server availability and RTO/RPO SLA failures occur in the same month Redcentric will pay service credits against whichever SLA failure gives the higher monetary value in service credits.

Claims for service credits must be made within 60 days of the service restoration.

7. Secure Data Import / Export Responsibilities and Accountabilities

7.1 High Level Redcentric Responsibilities

Redcentric is responsible for and will undertake the following activities:

- Connection of the customer supplied USB device to the Data Transfer Server within the platform at either site (the process for transporting and receipt of the USB device will be agreed with the Customer prior to commencing the data transfer process)
- Creation of a temporary Import Customer Virtual Machine if required to support data transfer to a Managed Physical Host
- Removal of the customer supplied USB device from the Data Transfer Server and return to the customer as per the agreed process

7.2 High Level Customer Responsibilities

To utilise the service, the following must be in place:

- The Customer workload, and virtual machines and/or Managed Physical Hosts that require the files\data must have completed the operational acceptance process and formal customer acceptance.
- Customer must provide a removable USB device that meets their security requirements for the transfer of data. (The Data Transfer Server supports USB 2 and USB 3 devices)
- Transport and collection of the USB device to/from the Redcentric Datacentres, including any associated power packs/adaptors
- Disposal and secure erasure of the USB device in accordance with the customer requirements.

Copying of the data from the USB device to the customer allocated storage including:

- Management of all encryption passwords
- Formatting the USB device to a suitable file system that can be read by the target operating system, i.e. FAT32, or EXT etc. Note FAT32 is recommended as this is compatible with Linux and Windows.
- Making all data on the USB device Read-only (This will ensure that the Redcentric Anti-Malware scanner does not delete/quarantine any customer data)
- Nomination of the target VM to copy the data to/from
- Transfer of the files to/from the customer nominated virtual machine

Customers can order the Redcentric Secure Direct Data Import and Export Service for a minimum period of half a day per site and is available in normal business hours from 8:00am to 6:00pm (UK time, Mon to Fri excluding UK holidays) or Out-of-Business Hours (all other times). See G-Cloud SFIA rate card for charges.

Secure Intelligent Hands are included as part of the Secure Data Import and Export Service.

For Secure Direct Data Import and Export Services, the customer must raise a service request via email or the customer portal in accordance with the agreed process at service take-on. Redcentric will use reasonable endeavours to schedule the use of the Secure Direct Data Import and Export service within 5 business days of a valid service request being received and acknowledged.

8. Business Continuity and Disaster Recovery

8.1 Business Continuity

Redcentric under its ISO22301:2019 Business Continuity certification, operates and maintains a robust Business Continuity Management System (BCMS). The BCMS scope includes;

- Data Centers
- Managed Services
- ICT technologies and systems
- Staff and business functions

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

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

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

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

Testing

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

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

Network resilience

Our network 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.

8.2 Disaster Recovery

8.2.1 Shared Platform Virtual Machines

Our standard shared platform virtual machines can be deployed in the following ways.

Dev and Test (Alpha/Beta) and Standard (Live) Virtual Machines

Option 1: Primary Site only: No Storage Replication.

Option 2: Primary Site with Secondary Site Storage Replication.

For option 2, in the event of the primary site becoming unavailable, Redcentric does not provide an RTO (Recovery Time Objectives) Service Level Agreement for these virtual machines at the secondary site and the recovery is carried out under reasonable endeavours.

For option 2, in the event of the primary site becoming unavailable, Redcentric will support an RPO (Recovery Point Objectives) down to a maximum of one hour at the secondary site for Dev and Test (Alpha/ Beta) and Standard (Live) Virtual machines.

8.2.2 High Availability (Live) Virtual Machines

Redcentric offers Sovereign High Availability (Live) virtual machines on the shared platform are provisioned with storage replication enabled by default and these virtual machine resources are both uncontended and reserved at the secondary site. Redcentric offers an RTO of four hours at the secondary site and an RPO down to a maximum of 1 hour for the recovery of High Availability (Live) virtual machines at the secondary site.

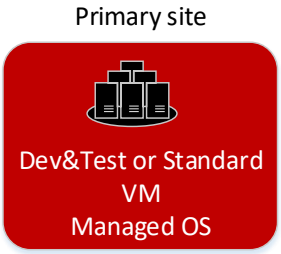
Lower RTO's and RPO's may be available upon request. To discuss this in more detail, please contact your account manager.

8.2.3 Shared Platform Virtual Machines – Workload Design Patterns

The following designs are illustrative and are examples only. Each design includes the number of virtual machine types, OS Licences, Managed Operating system instances and other elements that are required to support the design.

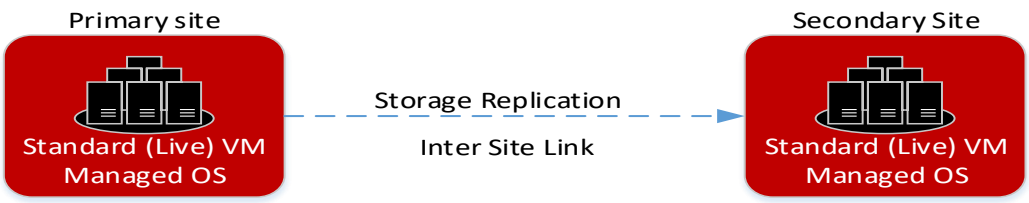
Dev and Test (Alpha/Beta) and Standard (Live) Virtual Machine - No Storage Replication

VM Type	Managed OS Licence	Replicated Storage	Example Workloads
One x Dev & Test or Standard VM	One	No	Build Server Pre-production Application server Load injection Server



8.2.4 Standard (Live) Virtual Machines – Replicated Storage

VM Type	Managed OS OS Licence	Replicated Storage	Example Workloads
Two x Standard VM	Two	Yes	Production Web Server Production Application Server.

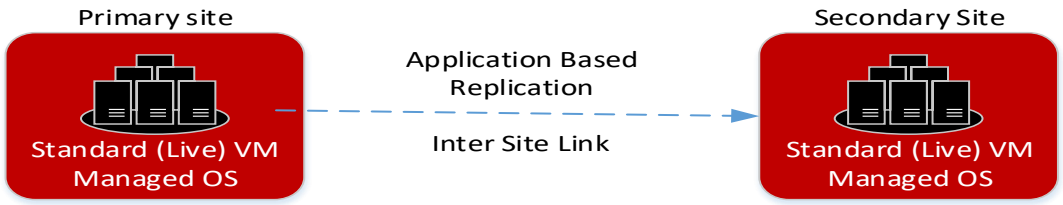


Note: Redcentric recommends that servers and services that require this set up can operate in an Active/Passive design pattern.

8.2.5 Standard (Live) Virtual Machines – Un-replicated Storage

VM Type	Managed OS Licence	Replicated Storage	Inter-site Bandwidth	Example Workloads
Two x Standard VM	Two	No	Yes	Active Directory Database Server

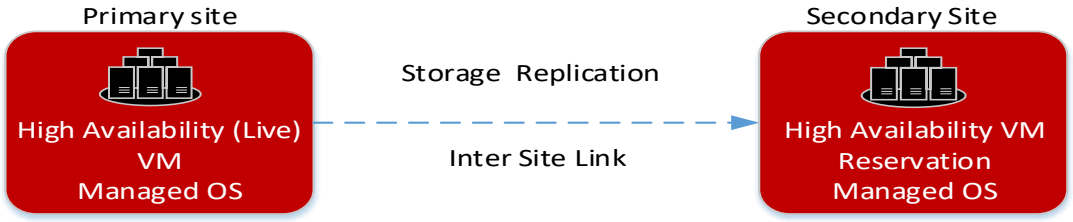
This design is appropriate for environments where downtime is highly undesirable or where application-based replication is preferable.



It is the customer's responsibility to implement application-level availability. Customer applications in an active-active configuration will leverage the inter-site resilient links between the data centres. Link bandwidth charges are based on reserved capacity.

8.2.6 High Availability (Live) – Replicated Storage

VM Type	Managed OS Licence	Replicated Storage	Example Workloads
One x High Availability VM	One	Yes (included)	Production Web Server Production Application Server



8.2.7 Managed Physical Hosts

For workloads that require physical servers, for example, performance or licencing reasons, Redcentric can provide Managed Physical Hosts. All server images and all other data for Managed Physical Hosts will be stored on data store(s) per customer on the available shared tiers of storage arrays, as is provided for our standard shared platform virtual Machine instances.

We will not provision local storage for Managed Physical Hosts or attach customer provided peripherals or interfaces to the devices. Redcentric will work with you to determine the server(s) specification you require to meet your application performance demands. Managed Physical Hosts can be deployed in Single Site or Dual Site configurations. Redcentric offers 3 Managed Physical.

8.2.8 Host Types

- Small Server: Single Socket 4 Core with 32 GB RAM

- Medium Server: Dual Socket 6 core with 64 GB RAM
- Large Server: Dual Socket 10 Core with 128 GB RAM
- Extra Large Server: Dual socket 40 Cores with 256GB RAM
- Memory Optimised Extra Large Server: Dual Socket 40 Cores with 768GB RAM
- Memory Extreme Extra-Large Server: Dual Socket 32 Cores with 4096GB RAM

Note: Managed Physical Hosts can only be ordered as part of a solution that includes standard shared platform virtual machines as detailed in Section 1.5 and are available for a minimum committed period of 12 months.

Managed Physical Hosts can be deployed in the following ways:

8.2.8.1 Single Site Single Server

A single server or number of single servers with dual power supply connected to redundant network and storage layers at the single site. This server has no resilience or fail-over. Replicated Storage can be included as part of Single Site Server deployments

8.2.8.2 Single Site with N+1 Cold Standby Server

One or more active servers with one or more local cold standby servers all with dual power supply connected to redundant network and storage layers. In a local cold failover configuration, the active server is shut down and its workload switched to a standby server which is then booted.

8.2.8.3 Single Site with N+1 Warm Standby Server

One or more active servers with one or more warm local standby servers all with dual power supply connected to redundant network and storage layers. In a local warm failover configuration, the active server and local warm standby server(s) have their own boot volumes (LUNs) so are independent and run concurrently. A second volume and LUN are created and presented to the primary server. The volume is replicated to the local warm standby server(s) but is inaccessible.

When failover is invoked, the volume becomes accessible to the warm local standby server. When the failover server is running, the volume will appear instantly as a new drive or mount depending on the Operating System.

8.2.8.4 Dual Site with N+1 Cold Standby Server

One or more active servers with one or more remote cold standby servers all with dual power supply connected to redundant network and storage layers. In a dual site cold failover configuration, the active server is shut down and its Service Profile switched to a standby server in the secondary site which is then booted against the replicated LUN.

One or more active servers with one or more warm remote standby servers all with dual power supply connected to redundant network and storage layers. In a dual site warm failover configuration, the active server and the warm standby server(s) in the secondary site have their own boot volumes (LUNs) so are independent and run concurrently. A second volume and LUN are created and presented to the primary server. The volume is replicated to the standby server(s) in the secondary site but is inaccessible.

When failover is invoked, the volume becomes accessible to the warm standby server in the secondary site. Since the failover server is running, the volume will appear instantly as a new drive or mount depending on the Operating System.

Note: For customers who have multiple applications running on Managed Physical Hosts, if a single standby server is ordered either in a single site configuration or a dual site configuration to facilitate a failover, then the standby server must have the same specification as the largest Managed Physical Host in terms of the number of Processors, CPU cores/speed and RAM.

8.2.8.5 Active:Active Servers

One or more servers with dual power supplies connected to redundant network and storage layers at the primary or secondary site. Multiple servers can be deployed to support higher levels of application or database availability, such as Oracle RAC Clusters, Microsoft SQL Server "Always on" Availability Groups or Microsoft Exchange Database Availability Groups. The redundant network is layer 3 encrypted. The servers write to the primary SAN storage which is then replicated to the remote SAN storage.

8.2.8.6 Dual Site with N+1 Warm Standby Server

On any configuration of Managed Physical Host(s) application(s), if there is a reliance on other services running on shared platform virtual machines then all such virtual machines would need to be failed over as well to support a complete failover solution and RTO to maintain a consistent running state. Managed Physical Host is only available as part of a PAAS service.

8.3 Operating System Templates

Redcentric will provide pre-hardened Operating System templates from which Redcentric will deploy your virtual machines and physical hosts. The template builds are in accordance with the National Cyber Security Centre (NCSC) guidelines and Public Service Network (PSN) requirements. We provide templates for the following operating systems.

OS Type	Version	Edition
Microsoft Windows Server	2016 R2 64 bit	Standard, Enterprise
Microsoft Windows Server	2016 R2 64 bit	Standard, Datacentre Edition
Linux	8 64 bit	Redhat Enterprise Linux
Linux	7 64 bit	Redhat Enterprise Linux

Redcentric will maintain the supported operating system templates. From time-to-time Redcentric will add new operating system templates.

9. Managed Operating System Services

9.1 Managed Operating System - Monitoring and Management

Managed Operating System - Monitoring and Management	
Service Description	The service provides customers with day-to-day monitoring and management of supported operating systems hosted by Redcentric. Aspects managed include OS availability and performance, software agents, and connectivity. The service provides applications for fixes where necessary and regular reporting.
Support Hours	Levels 1, 2
Service Dependencies	Service is provided for supported Microsoft and Red Hat Enterprise Linux only.
Monitoring Scope	Including CPU utilisation, memory utilisation, swap space utilisation, file system utilisation, log file monitoring, process monitoring, resource threshold alarms.
Agent Software Included	Monitoring, Management, Anti-Virus
Administrator Access Required	Yes.
Service Scope	This service provides the following: 24/7 monitoring of the OS for availability using appropriate tools. Monitoring and maintenance of backup/restore tasks and resource utilisation. Assistance with troubleshooting of agents and connectivity issues. Alert categorisation and incident escalation. Monitoring event logs, error reports, scheduled activities, and services, raising and tracking incident tickets as required. Application of hot fixes and service packs as per maintenance schedules. Management of server memory; optimisation and configuration of page files. OS hardening. Troubleshooting of OS performance issues. Performance reports (defined at service take-on).
Service Exclusions & Constraints	This service specifically excludes the following: Management of DNS, Active Directory and LDAP. Application monitoring. Applications covered by other optional Services: for example: IIS, MS SQL.

9.2 Managed Operating System - Anti-Virus

Managed Operating System - Anti-Virus	
Service Description	The service provides security protection against viruses through monitoring and management tasks.
Support Hours	Levels 1, 2.
Service Dependencies	Managed Operating System - Monitoring and Management.
Monitoring Scope	Anti-virus service will only be provided where the Operated systems are supported.
Agent Software Required	Monitoring, Management, Anti-Virus.

Managed Operating System - Anti-Virus	
Administrator Access Required	Yes.
Service Scope	This service provides the following: Initial installation and configuration of AV software on all managed Windows OS servers. Testing and verification of AV and system performance. Periodic assessment of maintenance and security updates. Maintenance and management of AV servers and updates of client servers. Monitoring and reporting on virus alarms; performance of file clean-ups. Monitoring of product updates and patches, and performance of regular analysis of critical security patches. Monitoring of CPU, memory, and hard disk drive (HDD) usage on the AV server as well as the AV console and clients. Performance of fixes on client systems. Root cause analysis and management of incidents for all virus-related calls, raising incidents where necessary. Regular AV console reports. Latest virus definitions for all systems.
Service Exclusions & Constraints	Service will only be provided on top of supported MS Windows Operating Systems. See Section 4 Managed Operating Systems.

9.3 Managed Operating System - Patch Management

Managed Operating System - Patch Management	
Service Description	The service provides patch management within an environment covered by the Managed Operating System Service.
Support Hours	Levels 1, 2.
Monitoring Scope	Status of managing agent and patch level.
Agent Software Included	Monitoring, Management, Anti-Virus.
Administrator Access Required	Yes.
Service Scope	This service provides the following: Management of OS files; quarterly assessment of software patches and service packs. Monitoring of product updates and priority patch alerts. Deployment of OS patches/updates. Risk assessment, testing, qualification, application and verification of patches for server software and standard builds. Management of the patching environment and tools. Production of regular patch reports.
Service Exclusions & Constraints	Service will only be provided where the Operating Systems are supported. See Section 4 Managed Operating Systems.

10. Managed Microsoft Application Services

10.1 Managed IIS - Monitoring and Management

Managed IIS	
Service Description	The service provides customers with day-to-day monitoring and management of supported Microsoft Internet Information Server instances. Aspects managed include web server availability and performance, software agents, and connectivity. The service provides applications for fixes where necessary and regular reporting.
Support Hours	Levels 1, 2
Service Dependencies	Service will be provided for supported MS Windows Operating Systems only.
Monitoring Scope	Including CPU utilisation, memory utilisation, swap space utilisation, file system utilisation, log file monitoring, process monitoring, resource threshold alarms.
Agent Software Included	Monitoring, Management
Administrator Access Required	Yes.
Service Scope	This service provides the following: 24/7 monitoring of IIS for availability using appropriate tools. Monitoring and maintenance of backup/restore tasks and resource utilisation. Assistance with troubleshooting of agents and connectivity issues. Alert categorisation and incident escalation. Monitoring of event logs, error reports, scheduled activities, and services, raising and tracking incident tickets as required. Application of hot fixes and service packs as per maintenance schedules. Troubleshooting of IIS performance issues. Performance reports (defined at service take-on).
Service Exclusions & Constraints	This service specifically excludes the following: Application monitoring.

10.2 Managed Active Directory Servers - Monitoring and Management

Managed Active Directory Servers	
Service Description	The service provides customers with day-to-day monitoring and management of supported Microsoft Active Directory Server instances. Aspects managed include Domain Controller and Directory Service server availability and performance, software agents and connectivity. The service provides application of fixes where necessary and regular reporting.
Support Hours	Levels 1, 2

Managed Active Directory Servers	
Service Dependencies	Service will only be provided on top of supported MS Windows Operating Systems
Monitoring Scope	Management and monitoring of trust relationships and AD security. Monitor and manage replication of the AD. Monitoring of event logs, error reports, scheduled activities, and services.
Agent Software Included	Monitoring, Management
Administrator Access Required	Yes.
Service Scope	This service provides the following: 24/7 monitoring of MS Active Directory Server(s) for availability using appropriate tools. Monitoring and maintenance of backup/restore tasks and resource utilisation. Assistance with troubleshooting of agents and connectivity issues. Alert categorisation and incident escalation. Monitoring of event logs, error reports, scheduled activities, and services, raising and tracking incident tickets as required. Application of hot fixes and service packs as per maintenance schedules. Troubleshooting of AD performance issues Addition/deletion/modifications of domain controllers as required; modify configuration of AD to reflect changes within the organization (for example new office). Management and administration of containers within the AD. Perform import/export of AD information in line with ad-hoc requirements, for example exports of the Global Address List (GAL). Performance reports (defined at service take-on).
Service Exclusions & Constraints	This service specifically excludes the following: User, Group and other Directory Administration

10.3 Managed Microsoft SQL Database - Monitoring and Management

Managed Microsoft SQL Database instances	
Service Description	The service provides customers with day-to-day monitoring and management of supported Microsoft SQL Server Database instances. Aspects include assuring the availability, performance and connectivity of the database instances. The service provides applications for fixes where necessary and regular reporting.
Support Hours	Levels 1, 2

Managed Microsoft SQL Database instances	
Service Dependencies	Service will only be provided on top of supported MS Windows Operating Systems.
Monitoring Scope	24/7 monitoring of database instances Monitoring and maintenance of backup/restore tasks and resource utilisation.
Agent Software Included	Monitoring, Management, Backup
Administrator Access Required	Yes.
Service Scope	This service provides the following: Validation of database backups Database user/role password management Add/remove/modify users to DB Security Configuration Addition, resizing and configuration of database files and objects Configuration of Database logical backups Configuration of Database initialization and tuning parameters Provision of DB copies (cloning) where required Configuration of Database Exports Configuration of monitoring tools for Database Resource thresholds Modification of Security Privileges Database & Table Management Memory Management Process Management Storage Management Session and Transaction Management using proactive monitoring toolset Creation and management of Database Management Tasks Backup/Restoration Performance Tuning Log Shipping Replication Application of hot fixes and service packs as per maintenance schedules

10.4 Managed Microsoft Exchange - Monitoring and Management

Managed Microsoft Exchange	
Service Description	The service provides customers with day-to-day monitoring and management of supported Microsoft Exchange Server instances. Aspects include assuring the availability, performance, and connectivity of the Exchange Server instances. The service provides applications for fixes where necessary and regular reporting.
Support Hours	Levels 1, 2

Managed Microsoft Exchange	
Service Dependencies	Service will only be provided on top of supported MS Windows Operating Systems
Monitoring Scope	24/7 monitoring of Exchange Server instances Monitoring and maintenance of backup/restore tasks and resource utilisation.
Agent Software Included	Monitoring, Management, Backup
Administrator Access Required	Yes.
Service Scope	This service provides the following: Perform continuous assessments of priority security patch updates Coordinate and participate in testing of Security Patches prior to production release Validation of Exchange Server backups Configuration of Exchange Server logical backups Configuration of Exchange Server initialization and tuning parameters Configuration of monitoring tools for Exchange Resource thresholds Modification of Security Privileges Memory Management Process Management Storage Management Session Management using proactive monitoring toolset Creation and management of Exchange Server Management Tasks Backup / Restoration Performance Tuning Replication Additions, deletions, and modifications to public folders and access rights to folders only as 3rd line of support with customer responsible for end user management activities. Management of public folders replication. Monitoring and management of Exchange log files, resolution of any issues caused by log files. Monitoring backup jobs to ensure that jobs have been completed and that log files have been cleared down. Management and support for the Messaging configuration – installation and configuration files, log files, messaging databases, and storage groups. Regular maintenance and defrag of messaging databases, repair, and recovery of databases to maximise system availability. Troubleshooting email delivery issues, NDRs (non-delivery receipts) from source to recipient. Management of Global Address List entries - custom recipients, mail forwarding, address book views, primary email address changes only as 3rd line of support with customer responsible for end user management activities.

Managed Microsoft Exchange	
	Managing mailboxes – implementation of mailbox policies and limits, moving of mailboxes between storage groups and/or servers. Producing regular and ad-hoc reports from the messaging infrastructure, using native reporting tools. Adding, configuring, modifying, and deleting mail domains within anti-spam & content filtering software. Blocking domains or addresses reported as known spammers. Management of quarantine and tag levels. Tool based Reporting on mail traffic volumes, spam volumes, etc. on a regular basis.

11. Managed Reverse Proxy Services

11.1 Managed Squid Proxy - Monitoring and Management

Managed IIS	
Service Description	The service provides customers with day-to-day monitoring and management of Virtual Machines running Squid proxy services. Managed aspects include virtual machine availability, performance, software agents and connectivity. The service provides applications for fixes where necessary and regular reporting.
Support Hours	Levels 1, 2
Service Dependencies	Service will only be provided on top of supported Red Hat Enterprise Linux
Monitoring Scope	Including CPU utilisation, memory utilisation, swap space utilisation, file system utilisation, log file monitoring, process monitoring, resource threshold alarms.
Agent Software Included	Monitoring, Management
Administrator Access Required	Yes.
Service Scope	This service provides the following: 24/7 monitoring of proxy for availability using appropriate tools. Monitoring and maintenance of backup/restore tasks and resource utilisation. Assistance with troubleshooting of agents and connectivity issues. Alert categorisation and incident escalation. Monitoring event logs, error reports, scheduled activities, and services, raising and tracking incident tickets as required. Application of hot fixes and service packs as per maintenance schedules. Troubleshooting of performance issues. Performance reports (defined at service take-on).
Service Exclusions & Constraints	This service specifically excludes the following: Application monitoring.

12. Data Processing

12.1 Personal Data Processing Statement

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

12.2 Subject matter of the processing

Provision of support service for customers utilising Amazon Web Services Cloud with optional professional services.

A service desk with second- and third-line support is included.

12.3 Nature and purposes of the processing

All personal data is stored in UK Data. It will be necessary to store CCS 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 CCS Customer Contract.

12.4 Duration of the processing

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

12.5 Categories of Data Subject

CCS Customer Commercial, Account, Technical, and Finance personnel.

12.6 Categories of Data Subject International Transfers

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

12.7 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.

12.8 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).

12.9 Special Category Data

No special category data is accessed by Redcentric personnel.

12.10 Data Processing Location

Data Processing location is the UK.

13. Exit Plan

13.1 End of contract data extraction

On termination or expiry of the Service Agreement, customers are responsible for the extraction on any data required beyond the end of the contract.

13.2 End of contract additional assistance

Where the Customer requests additional transitional assistance, Redcentric shall provide such assistance as an additional service. The additional transitional assistance shall be chargeable at the Redcentric prevailing time and materials consultancy day rates.

13.3 Resource Deletion

The customer is responsible for deletion of self-service resources. Redcentric will delete managed resources at the end of the contract unless an extension has been requested. In either case, consumed resources will continue to be charged at the contracted rate.

14. Managed Detection & Response Service

14.1 Customer Asset Protective Monitoring

Redcentric and its key service partners (collectively "the Supplier") provides a Managed Detection and Response (MDR) service, with 24/7/365 cyber security threat detection and response.

The service captures and alerts on events commensurate to the data processing requirements of each environment, as stipulated by the PSN Code of Connection and the recommendations laid out by the National Cyber Security Centre (NCSC).

14.2 Service Features

Security monitoring is provided by the Supplier's UK-based 24/7 Security Operations Centre. The Supplier will provide a security managed service (Managed Cyber Security Operations Service), supporting threat detection, triage, investigation, incident response, compliance reporting through the collection and analysis of computer-generated alarms from historical data across a variety of sources and this may include the partial or full remediation of an identified threat.

The service encompasses the end-to-end management of alerts and security events relating to potentially malicious cyber activity which includes, at a high-level:

- Implementation and/or configuration management of SIEM, EDR, and SOAR tooling.
- Provisioning access to the Supplier's ITSM / Case Management system for Customers and nominated Redcentric personnel.
- Identification and triage of security events and alerts generated via the Customers SIEM.
- Remote investigation and response to identify and where agreed (as per the authority to act) contain and eradicate security threats.
- Escalation of security issues that cannot be resolved independently, engaging the Supplier's Retained Incident Response services where required.
- Continuous development and tuning of alert logic and response playbooks.

14.3 Out-of-scope

The following components are considered out of scope and will be performed by Redcentric or a third-party Supplier:

- Deployment and ongoing management of EDR, AV, EPP, IDS, IPS, Firewall, or any security technology other than SIEM/SOAR.

14.4 Service Tiers

The managed service is provided with the following options:

- **Managed Detection and Response (MDR)** – MDR primarily focuses on threats within individual systems and devices. MDR is only applicable in situations where the service is based on telemetry from the endpoint estate as the core detection surface (laptops, phones, PCs, servers, access points, routers and firewalls). Response will only be performed on servers and workstations, though telemetry may be ingested from other sources.
- **Managed eXtended Detection and Response (MXDR)** – Includes the coverage of MDR in addition to integrating and correlating data from various sources, such as network traffic, cloud environments, and email. XDR is designed to detect and respond to threats that move across different platforms and environments, providing a more holistic approach to cyber security. **The majority will fall into this bracket.**

Customers will select one of the following service tiers: MDR or MXDR, as per the table below.

Table: Service Summary

Stage	Feature / Service	Service Tier	
		MDR	MXDR
Initial Setup	Access / Build Client Azure Log Analytics Workspace	✓	✓
	Access / Build Client Microsoft Sentinel Workspace	✓	✓
	Connection Of Microsoft Lighthouse and Azure AD B2B	✓	✓
	Connection To Case Management	✓	✓
	Connection To Security, Orchestration Automation and Response (SOAR)	✓	✓
Deployment	Data Connector Build – Microsoft Cloud Data Connectors	✓	✓
	Data Connector Build – External Non-Microsoft [1]	Optional	Optional
	Deployment of the Supplier Analytic Library	✓	✓
	Custom Connector Development	Optional	Optional
	Custom Content Development	3	6
Management and Monitoring	Triage: Validation And Priority Evaluation	✓	✓
	Investigation: In-Depth Investigation on Multi-Stage Attacks Taking Appropriate Action E.G. Threat Hunting	✓	✓
	Containment: Execution Of Mitigation Procedures to Manage True Positives in Line With The Authority To Act And Approved Security Technologies	✓	✓
	Continually updated from the Supplier Analytic Library	✓	✓
	Incident Management	×	✓
	Security Orchestration Automation Response	✓	✓
	Incident Response Playbooks	✓	×
	Tailored Incident Response Playbooks	×	✓
	Post Deployment Incident Response Tabletop Exercise	×	✓
	Shared Intelligence	✓	✓
	Managed Intelligence[2]	×	×
	Customer Portal Access	✓	✓
	Threat Hunting[3]	✓	✓
Deception Technologies	Microsoft Defender for Endpoint Deception	×	✓
Continuous Improvement	Custom Content Per Quarter	5	10
	Root Cause Analysis of True Positive P1	×	✓

1 Based upon the Supplier's existing connector library.
2 Managed Threat Intelligence is an optional add-on.
3 Hunts based upon behaviours and indicators of compromise from Shared Intelligence
4 Subject to agreement with the Supplier and resource availability

14.5 Deployment Options

Two options will be offered for deployment:

- Standard – a streamlined deployment model in line with a standardised scope with a level of acceptable deviation from the standardised connectors, technologies, service levels, and Authority to Act actions.
- Customised – a custom deployment involving deviation from the standardised model, due to the complexity of the environment or business requirements.

A deployment and on-boarding programme typically takes around 8 weeks. Custom deployments may take longer and will be estimated during initial scoping and revisited following commencement of the on-boarding programme. Lead times for on-boarding are approximately 4 weeks from contract signature and acceptance.

14.6 Ancillary Services

The following additional components will also be included for Customers of the service:

- All Customer contracts will include an individual Incident Response Retainer unless they decide to opt out (e.g. in the event they already have a relationship with an IR provider).
- All Customer contracts will include fees for the maintenance and continuous development of the Supplier's service management tooling (exc. human resource costs).

14.7 Pre-requisites

The Customer should have the following to be able to take on the service:

- An existing EDR deployment across the entirety of their endpoint estate that is in scope for the service (ideally Microsoft Defender for Endpoint but alternative EDRs can be supported).
- If planning to use Microsoft Sentinel as the SIEM, an existing billing relationship with Microsoft.

14.8 Service Variants

In some cases, the service may be adjusted based on the Customer's business and network context. For example:

- Where the SOC remit ends with notifying the Customer due to a lack of permission (via the Authority to Act) or access (due to the environment being locked down with no ability to interact with the endpoint). In this scenario the onus for further triage and investigation of an event would be on the Customer.

These adjustments will not result in any reduction to the cost per unit but may incur additional costs in particularly non-standard or complex environments.

14.9 Standard Deployment

14.9.1 Initial Setup & Deployment

- The Supplier will appoint a Project Manager (PM) to co-ordinate the Initial Setup & Deployment. All work and activity of any The Supplier resources supporting the Initial Deployment & Setup will be undertaken remotely.
- The Supplier will provide the Customer with standard deployment and architecture documentation to support the Initial Setup & Deployment.
- The Supplier will deploy Microsoft Sentinel and Log Analytics into the Customer's Tenant; or where a Microsoft Sentinel deployment exists.
- The Supplier will review the configuration of Microsoft Sentinel against industry best practice.

- The Supplier will connect to the Customer's Tenant with Microsoft Lighthouse.
- The Supplier will enable access to the Customer's Tenant for SOAR.

14.9.2 Pre-requisites

The following services will be available or in place that will connect to the Supplier Managed Cyber Security Operations Services and are necessary for the service to function and will ensure that these services meet any minimum technical requirements that the Supplier specifies.

- Microsoft Sentinel and Log Analytic Workspace (each an "Enabling Service")

To provide the Sentinel and or XDR service, the Supplier will also require access to Customer tenants that provide your user and infrastructure protection using the Microsoft Defender suite of services.

The Supplier will be granted access to the appropriate services within your Tenant to enable the creation and ongoing management of the Managed Cyber Security Operations Service.

14.9.3 Optional add-ons

The Customer may request that, at an additional Charge, resources will be available to attend meetings at your Site as is reasonably required, depending on your location, for the duration of the Initial Setup & Deployment.

The Supplier may provide you with Professional Services at an additional Charge, at your request, to assist you in the deployment and integration of the following technologies:

Microsoft Defender for Endpoint | *Microsoft Defender for Collaboration | *Microsoft Defender for Cloud | *Microsoft Defender for Identity | *Microsoft Entra ID | *Microsoft Purview | *Microsoft Defender for Identity | *Microsoft Defender for IoT | *Microsoft Security Co-Pilot | Corelight NDR

*Microsoft technology names may change from time to time and The Supplier will support future versions of the named technologies above.

The Supplier may provide the Customer with Professional Services at an additional Charge, at your request, to assist the Customer with the following areas:

- The creation of your Custom Content.
- The integration of Data Sources.

14.9.4 Content Design and Deployment

The Supplier will provide the Customer with all applicable Microsoft Sentinel analytics from the Repository.

Should the Supplier elect to standardise Custom Content requested by the Customer/Redcentric, the content will be added to the Repository, made available to The Supplier's wider Client base, in which case the content will cease to count towards your Custom Content allocation and no additional Charges will apply. In such circumstances, The Supplier will own the Intellectual Property Rights in relation to the content.

Subject to receiving acceptable information from the Data Sources, the Supplier will configure the Managed Cyber Security Operation Service to implement the Custom Content agreed.

14.9.5 Data Source Connection

The Supplier will configure the Managed Cyber Security Operations Service to receive Event Log Data from the full Microsoft technology Data Sources using the default Microsoft connectors. This includes but is not limited to:

- Microsoft Defender for Endpoint
- Microsoft Defender for Collaboration
- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- Microsoft Entra ID
- Microsoft Purview
- Microsoft Defender for Identity
- Microsoft Defender for IoT
- O365 Activity Logs
- Azure Activity Logs
- Exchange Online

The Supplier will configure the Managed Cyber Security Operations Service to receive Event Log Data from the Data Sources agreed with you and set out in any applicable Statement of Work.

The Customer will configure the Data Sources to send Logs to the Managed Cyber Security Operations Service or provide The Supplier with the requisite details and consents to enable the Supplier to configure the Data Sources directly, as set out in any applicable Statement of Work.

The Supplier will only undertake monitoring and management of Data Sources that are set out any applicable Statement of Work.

14.9.6 Early Life Service

Upon completion of Initial Setup, The Supplier will transition the Managed Cyber Security Operations Service into “Early Life Service”.

The Supplier will work with the Customer and Redcentric to agree an Escalation Matrix for use during Early Life Support.

The Supplier will provide access to the Supplier Portal.

During Early Life Service, The Supplier will:

- Deliver a 24x7 threat detection service consisting of triage and investigation of computer-generated alarms from Microsoft Sentinel. During Early Life Service,
- Work with the Customer to appropriately tune security alarms.
- Continue to develop and deploy any Custom Content and Connectors agreed in any Statement of Work.

The Supplier will provide the Customer with a Security Operations Manual which will be completed during the Early Life Service Period and will include the Authority to Act.

14.10 Supplier Portal

The Supplier grants to the Customer during the Term a non-exclusive, royalty free, license to access and use the Supplier Portal solely to the extent necessary to receive the Services and in compliance with The Supplier’s acceptable use policy for such portal in force from time to time.

Ownership of all Intellectual Property Rights in the Supplier Portal remains with the Supplier and nothing in the Statement of Work will operate to transfer to the Customer or to Redcentric or to grant to the Customer any other license or right to use the Supplier Portal.

The Supplier may at its absolute discretion, upon written notice, suspend the Customer's access to the Supplier Portal at any time if the Client uses the Supplier Portal in breach of the Agreement or the applicable acceptable use policy.

The Customer shall ensure that its access credentials for the Supplier Portal are stored securely and only used by authorised employees and are not shared with any other person. The Customer shall take all reasonable steps to prevent any unauthorised access to the Supplier Portal and will immediately notify the Supplier if it becomes aware of any such access;

The Supplier Portal will provide the Customer with a central database of historic events, incidents and performance. This data will be exportable for Customer use.

14.11 Acceptance into Service

Upon completion of Early Life Support, the CSM and the Client will agree a date for Acceptance into Service. Upon Acceptance into Service the agreed Service Levels will come into effect. Acceptance Criteria include the completion of:

- Microsoft Sentinel deployments
- Microsoft Lighthouse connection
- The Supplier SOAR connectivity
- The Supplier Portal access enabled
- Deployment of the relevant content from the Analytic Library
- Deployment of the agreed Custom Content and Connectors
- Tuning of content
- Escalation Matrix
- Security Operations Manual including but not limited to;
    a. Authority to Act
    b. Incident Response Playbooks
    c. Escalation Matrix

Incident Response Tabletop Exercise as applicable to the Service Tier.

Delivery of the Exit Plan

14.12 Default Authority to Act

Customers will receive a default Authority to Act as per the table below. Deviations from this Authority to Act will be chargeable as per the "Customised" deployment model.

Table: Default Authority to Act

Action	Approved for Managed Service?	Approved for Incident Response?	Supported Products	Title
Get information about a specific host, existing vulnerabilities, or about vulnerabilities it had at a particular time in the past	Rejected	Rejected	['M365Defender', 'Tenable']	RA_2002_list_host_vulnerabilities
Contact relevant 3rd parties to share indicators and collaborate	Rejected	Approved	['No Current Supported Products']	RA_2130_contact_3rd_party
List users that have opened an email message	Approved	Approved	['No Current Supported Products']	RA_2201_list_users_who_have_opened_email_message

Action	Approved for Managed Service?	Approved for Incident Response?	Supported Products	Title
Collect an email message	Approved	Approved	['O365ATP']	RA_2202_collect_email_message
Collect a specific file from a (remote) host or a system	Approved	Approved	['M365Defender', 'CrowdStrike']	RA_2311_collect_files
Collect an investigation package	Approved	Approved	['M365Defender']	RA_2321_collect_investigation_package
Contact the user to provide guidance, notification or seek details.	Approved	Approved	['Microsoft Teams', 'Email']	RA_2701_contact_user
Patch a vulnerability in an asset	Rejected	Rejected	['No Current Supported Products']	RA_3001_patch_Vulnerabilities
Block an external IP address from being accessed by corporate assets	Rejected	Approved	['M365Defender']	RA_3101_block_external_ip_address
Block an internal IP address from being accessed by corporate assets	Rejected	Approved	['No Current Supported Products']	RA_3102_block_internal_ip_address
Block an external domain name from being accessed by corporate assets	Rejected	Approved	['M365Defender']	RA_3103_block_external_domain
Block an external URL from being accessed by corporate assets	Approved	Approved	['M365Defender']	RA_3105_block_external_url
Block a network port for external communications	Rejected	Approved	['No Current Supported Products']	RA_3107_block_port_external_communication
Block a network port for internal communications	Rejected	Approved	['No Current Supported Products']	RA_3108_block_port_internal_communication
Block a user for external communications	Rejected	Approved	['No Current Supported Products']	RA_3109_block_user_external_communication
Block an email sender on the Email-server	Approved	Approved	['O365ATP', 'Mimecast']	RA_3202_block_sender_on_email
Quarantine an email message	Approved	Approved	['O365ATP']	RA_3203_quarantine_email_message
Mark and notify a reported email message. This provides end user feedback for reported email submissions.	Approved	Approved	['O365ATP']	RA_3204_mark_and_notify_reported_email
Quarantine a file by its hash	Rejected	Approved	['M365Defender', 'automation']	RA_3302_quarantine_file_by_hash
Block a process execution by its executable hash	Rejected	Approved	['M365Defender']	RA_3403_block_process_by_executable_hash
Quarantine a device to prevent access to other network resources	Rejected	Approved	['M365Defender']	RA_3410_quarantine_device
Disable a system service	Rejected	Approved	['Powershell']	RA_3501_disable_system_service
Create a live response session in EDR tooling.	Approved	Approved	['M365Defender']	RA_3511_initiate_live_response
Lock an user account	Rejected	Approved	['AzureAD', 'AD']	RA_3601_lock_user_account

Action	Approved for Managed Service?	Approved for Incident Response?	Supported Products	Title
Acquire a forensic copy of a virtual or physical disk	Rejected	Approved	['Azure']	RA_3904_acquire_disk_image
In the event of an incident where we are unable to contact the relevant stakeholders for approval should we bypass the a2a to prevent harm. This action would only be approved under incident by a Team Lead or SoC Manager.	Rejected	Rejected	['No Current Supported Products']	RA_3905_bypass_a2a
Acquire a forensic copy of running memory	Rejected	Approved	['No Current Supported Products']	RA_3906_acquire_memory_dump
Delete an email message from an Email Server and users' email boxes	Rejected	Approved	['O365ATP']	RA_4201_delete_identified_email_message
Remove a specific file from a (remote) host or a system	Rejected	Approved	['M365Defender', 'Powershell']	RA_4301_remove_file
Remove a registry key	Rejected	Approved	['M365Defender', 'Powershell']	RA_4501_remove_identified_registry_keys
Remove a service	Rejected	Approved	['M365Defender', 'Powershell']	RA_4502_remove_identified_services
Remove any malicious mailbox rules identified	Approved	Approved	['O365ATP']	RA_4503_remove_mailbox_rules
Remove any malicious Oauth apps that have been identified	Rejected	Approved	['AzureAD', 'DefenderForCloudApps']	RA_4504_remove_oauth_consents
Revoke authentication credentials	Rejected	Approved	['AzureAD', 'AD']	RA_4601_revoke_authentication_credentials
Remove a user account	Rejected	Approved	['AzureAD', 'AD']	RA_4602_remove_user_account
Report incident to abuse contacts to facilitate a takedown of the site or material	Rejected	Rejected	['No Current Supported Products']	RA_4610_takedown_site
In the event of a lost or stolen device if we are able to obtain a live response session, we can wipe the TPM chip which will force a bitlocker recovery.	Rejected	Approved	['M365Defender']	RA_4620_bitlocker_force_recovery
Run Anti-Virus scan on all impacted systems	Approved	Approved	['M365Defender']	RA_4901_run_anti-virus_scan
Unblock a blocked IP address	Rejected	Approved	['M365Defender']	RA_5101_unblock_blocked_ip
Unblock a blocked domain name	Rejected	Approved	['M365Defender']	RA_5102_unblock_blocked_domain
Unblock a blocked URL	Rejected	Approved	['M365Defender']	RA_5103_unblock_blocked_url
Unblock a blocked port	Rejected	Approved	['No Current Supported Products']	RA_5104_unblock_blocked_port
Unblock a sender on email	Rejected	Approved	['No Current Supported Products']	RA_5202_unblock_sender_on_email

Action	Approved for Managed Service?	Approved for Incident Response?	Supported Products	Title
Restore a quarantined email message	Rejected	Approved	['O365ATP']	RA_5203_restore_quarantined_email_message
Restore a quarantined file	Rejected	Approved	['No Current Supported Products']	RA_5301_restore_quarantined_file
Unblock a blocked process	Rejected	Approved	['No Current Supported Products']	RA_5401_unblock_blocked_process
Enable a disabled service	Rejected	Approved	['Powershell']	RA_5501_enable_disabled_service
Unlock a locked user account	Rejected	Approved	['AzureAD', 'AD']	RA_5601_unlock_locked_user_account
Un-Quarantine a device to restore access	Rejected	Approved	['M365Defender']	RA_5602_remove_devices_from_quarantine
The Supplier content development team to implement suppression of the alert to prevent false+ from re-occurring.	Approved	Approved	['M365Defender', 'Crowdstrike', 'Azure']	RA_6020_implement_alert_suppression

14.13 Customised Deployment

Customised deployment will be scoped and priced on a case-by-case basis based on the level of customisation and deviation from the standard model required.

Standard approval and deployment timescales will not apply in the case of customised deployments.

14.14 Service Delivery

14.14.1 Monitoring and Management

The Monitoring and Management will commence in full, from the agreed Acceptance into Service date. The Supplier will proactively monitor and manage the Managed Cyber Security Operations Service 24x7x365.

14.14.2 Proactive Monitoring

The Supplier will establish a mutually agreed process to make contact when the Supplier identifies an issue that impacts the Managed Cyber Security Operations Service.

The Supplier will deliver the performance of the Managed Cyber Security Operations Service in line with the agreed Service Levels and, where possible, provide advance incident alert warning to the Customer and Redcentric through the Managed Cyber Security Operations Service, or via email, of impending issues that The Supplier identifies as a result of the monitoring. The Supplier may not identify all impending issues.

The Supplier will perform, in line with the service tier, all agreed actions within the Authority to Act prior to providing the advanced incident alert.

14.14.3 Containment and Eradication

Following the provision of an incident alert, the Supplier will automatically implement any Response Action necessary, which has been previously agreed within the Authority to Act and Playbooks in respect to the applicable Playbook. The Supplier shall not be responsible for any impact on any Devices, Equipment, or the Customer's wider Network as the result of executing an agreed Response Action. The Supplier does

not make any representations or warranties, whether express or implied, as to any outcomes of Response Action.

Where the Customer wish for the Supplier to take a Response Action, but do not wish for The Supplier to automatically take such Response Action, you may specify that the Supplier is to instead seek your prior approval before implementing any Response Action within the Authority to Act.

14.14.4 Digital Forensics and Incident Response

The Supplier may provide Digital Forensics and Incident Response at an additional Charge, at the Customer's request, to assist in the containment and eradication of a threat that is outside the scope of the service.

14.14.5 Missing Log Source Monitoring and Reporting

The Supplier will notify the Customer, as soon as possible, if one or more of the Data Sources, fails to forward Event Log Data to the Managed Cyber Security Operations Service.

14.14.6 Security Event Management

Logs will be stored in relevant tables.

The Supplier will run Scheduled Rules against the relevant tables and categorise each Alarm raised according to its severity for inspection by the Supplier SOC.

The Supplier will search Events in accordance with the deployed analytic library and any agreed Custom Content.

The Supplier will analyse Event / Incident data generated by the Managed Cyber Security Operations Service.

The Supplier will assess and recommend appropriate remediation actions to be taken.

14.14.7 Security Incident Management

The Supplier will update the ticket of possible Security Incidents, including details of the relevant underlying Event and threat intelligence.

The Supplier will, if necessary, alert you via email, or as agreed, to any potential threats and/or action to be taken by you.

Based upon the service tier and the Authority to Act, the Supplier will contact your nominated contact/3rd Party to:

- advise of any necessary remedial action they need to take; and
- confirm that they have completed any necessary remedial action,
- following which the Supplier will close the ticket.

If the nominated Customer or Redcentric team does not take the necessary remedial action, the Supplier will not be responsible for the ongoing effects of the Security Incident.

Upon the closure of any true positive Priority 1 ticket the Supplier will offer RCA support and guidance on preventing the recurrence of Security Incidents. This advice may include:

- advising on malware related to a botnet, known to use command and control servers, that your devices have attempted to connect to; and
- advising on blocking certain defined network traffic or specific Twitter feeds, at firewall, proxy, or other appropriate control point.

14.14.8 Deception Technologies

The Supplier will provide an initial deployment, as agreed, of the Microsoft Defender for Endpoint Deception technologies.

The Supplier will, no more than once a quarter, as agreed, review the configuration of the Microsoft Defender for Endpoint Deception technologies.

14.14.9 Approved Security Technologies

The following Security Technologies are approved, as standard for Response Actions to be undertaken by the Supplier in the Managed Cyber Security Operations Service.

Technology Type	Service Tier	Vendor and Technology
Endpoint Detection and Response (EDR)	All	Microsoft Defender for Endpoint Microsoft Defender for Servers Crowdstrike EDR Sentinel One EDR Palo Alto XSOAR EDR Carbon Black EDR
Email Security	MXDR	Microsoft Defender for Collaboration Proofpoint Mimecast
Extended Detection and Response (XDR)	MXDR	Microsoft XDR
OT Monitoring	MXDR	Microsoft Defender for IoT
Network Monitoring	All	Microsoft Defender for IoT Corelight NDR

The Supplier may include additional Security Technologies, with a Charge and at the Customer's request, as agreed in any Statement of Work.

14.15 Continuous Improvement

Redcentric will provide the customer with a monthly report, focusing on the performance of the Managed Cyber Security Operations Service against service targets.

The Redcentric Service Delivery Manager (SDM) will hold a conference call to discuss the monthly report.

The Redcentric team will discuss the effectiveness of the Custom Content applied and the need to fine tune or amend the Custom Content.

The customer will take appropriate action to address issues in respect of fine tuning or amending your Custom Content as recommended by the Redcentric SDM.

Redcentric will implement changes to the Custom Content subject to the following process:

The authorised Redcentric contact will submit requests to change the Custom Content via a portal service request to the Supplier SOC, providing sufficient detail, and clear instructions as to any changes required, are provided.

Redcentric will check each request for its complexity and assess whether the change should be completed via the Content Change Management Process or whether it requires to proceed in accordance with Clause 6 (Changes) of the Agreement.

Simple Changes subject to the Reasonable Use Policy included in the Charges.

Complex Change requests will require a new Statement of Work under the Agreement and the Supplier will charge you the cost of implementing Complex Changes.

Redcentric may provide Professional Services at an additional Charge, upon request, to assist in writing the change request; and

Redcentric will apply the following “reasonable use” restrictions (“Reasonable Use Policy”) for changes to the Custom Content:

- Standard Change requests will not be raised more frequently than the frequency defined in the table in Section 14.17 per each end-customer.
- Where the Custom Content allocation defined in the table in Section 14.17 is not used, it does not carry forward.
- Urgent Change requests shall not be raised more frequently than three per quarter.

Where the Supplier’s measurements show that change requests are being raised more frequently than as set out in Section 14.17 the Supplier may, either:

1. aggregate the requests over a period, so that they may be implemented more efficiently. In this event there may be some implementation delays; or
2. review the requirements and agree an appropriate alternative implementation process and any associated charges.

The Supplier will use reasonable endeavours to implement an Emergency Change as quickly as is reasonably practicable. The Supplier may charge the cost of implementing an Emergency Change.

The Supplier may implement an Emergency Change without approval if deemed necessary to protect the service or its clients.

Redcentric and the Customer are deemed to have approved all changes to the Custom Content that you submit to The Supplier.

The Supplier will use reasonable endeavours to identify errors or potential unforeseen consequences of your requested Simple Changes and Complex Changes and advise you appropriately and will not be liable for any consequence arising from:

- miss-specification of security requirements in relation to the Custom Content; or
- unforeseen consequences of a correctly specified and correctly implemented Custom Content.

The Customer will be responsible for the impact of The Supplier implementing the changes and The Supplier is not liable for any consequences arising from the impact of the implementation of the changes.

14.16 Health Monitoring

The Supplier will perform transaction level monitoring to ensure the performance and availability of the security platforms are monitored. Every 5 minutes an alarm is generated and tracked through the systems to the eventual creation of a corresponding alert in Sentinel. This enables the identification of when and where a backlog or fault exists anywhere within the stack. When alerted, these faults will be raised with Microsoft by The Supplier with detailed information regarding effected regions and the exact location of the bottleneck.

For each log source the Supplier will record a performance baseline of the consumed log rate calculated from the hourly average over the last 7 days. When the behaviour of an active log source in Microsoft Sentinel has its standard logging levels deviate up or down by more than 30% over its baseline it triggers a Sentinel analytic.

- 30% Increase = Cost Alert
- 30% Decrease = Potential Loss of Logs Alert

Depending on the system/software that has deviated, different priorities can be agreed for the alert and the SOC will execute pre-agreed actions or escalate to the responsible customer team for further attention.

14.17 Health Service Levels Specific to the MDR Service Option

The Service Level Agreements below are applied across all alarms by default from Acceptance Into Service. Underperforming Custom Content that generate noise or have a high wastage value will be excluded until tuned.

14.17.1 Service Measurement Definitions

Table: Priority Definitions

Priority	Definition	Example
P1 (Critical)	These incidents will usually cause the degradation of vital service(s) for many users, involve a serious breach of cyber security, affect mission critical equipment or services or damage public confidence in the organisation.	Targeted cyber security attacks or loss of publicly available online service.
P2 (Significant)	Less serious events are likely to impact a smaller group of users, disrupt non-essential services and breaches of a security policy.	Website defacement or damaging unauthorised changes to a system.
P3 (Minor)	Many minor types of incident can be capably handled within the Detection and Response technology. All events are monitored and tracked for occurrences of similar events. This will improve understanding of the cyber security challenges and may raise awareness of new attacks.	Unsuccessful denial-of service attack or the majority of network monitoring alerts.
P4 (Negligible)	It is not necessary to report on incidents with little or no impact or those affecting only a few users, such as isolated spam or antivirus alerts.	Isolated anti-virus alert or spam email.

Table: Service Measurement Definitions

Term	Definition
"Acknowledgement Time"	Also known as “Mean Time to Acknowledge” or aligned to “Mean Time to Investigate”, is the time elapsed between ticket creation and the first touch by a human or a SOAR playbook.
"Response Time"	Also known as “Mean Time to Respond” is the time elapsed between ticket creation and the ticket closure time, minus an “lag” time such as “time on hold” or “awaiting feedback”

14.17.2 Service Level Agreements

Table: Service Level Agreements

Priority	Service Tier	Measurement	SLA (Mins)	Service Threshold
Priority 1 (Critical)	MDR	Acknowledgement	60	95%
		Response	240	
	MXDR and CSOC	Acknowledgement	30	
		Response	240	
Priority 2 (High)	MDR	Acknowledgement	120	97%
		Response	480	
	MXDR and CSOC	Acknowledgement	60	
		Response	480	

Priority	Service Tier	Measurement	SLA (Mins)	Service Threshold
Priority 3 (Medium)	MDR	Acknowledgement	240	97%
		Response	1440	
	MXDR and CSOC	Acknowledgement	120	
		Response	1440	
Priority 4 (Low)	MDR	Acknowledgement	480	97%
		Response	2880	
	MXDR and CSOC	Acknowledgement	240	
		Response	2880	

14.17.3 Service Credit Mechanism

Where services fail to meet the stated Service Level Threshold, service credits will be paid as a credit in the next monthly billing period. The maximum credits payable in the measurement period (measurement period being defined as a Calendar month) is 10% of the fixed charges payable in the measurement period (one off charges or professional charges are excluded from the charges used to calculate the service credit payable). The monetary value of any service credits will be deducted from the next service invoice.

Table: Service Credits

Priority	SLA Achievement Threshold	Percentage of Service Credits payable
P1	95%	4%
P2	97%	3%
P3	97%	2%
P4	97%	1%

For SLA categories P3 or below, where the occurrence of a failure in meeting the SLA due to low ticket volume, shall be subject to consideration for exclusion. The Supplier may initiate an exclusion request by providing notice to the other party. Upon receipt of the exclusion request, both parties agree to enter good faith discussions to assess the validity of the request and determine whether exclusion is warranted.

14.18 Service Access and Visibility

14.18.1 Accessing the Service

This document assumes that the chosen SIEM is Microsoft Sentinel.

The Customer accesses the service via the Customer Portal, and through their chosen SIEM. Access to the service is provided through the Customer Portal.

14.18.2 Case Management

The Supplier uses a dedicated case management system that directly integrates with the SIEM and The Supplier SOAR platforms. It is possible for Customer employees to access their Microsoft Sentinel dashboards at any time for their own investigation, visibility or to collaborate in real-time with analysts and responders via the Customer Portal. Further channels for collaboration will be through agreed channels, such as email and Microsoft Teams.

All tickets are managed through a single pane of glass, with each incident handled based on its priority.

- **Alarm:** A ticket automatically generated by Custom Content or Analytics from the Repository.
- **Incident:** A single unwanted or unexpected security event, or series of events, consisting of the actual or potential (attempt underway) exploitation of an existing vulnerability, and that has a significant probability of compromising business operations and threatening information security.

Priority is initially determined by set variables within integrated security products which, following triage, an analyst can overrule and modify based on their views.

Once an analyst has been assigned the ticket, they begin to conduct initial triage. The events associated to the alert are investigated with the goal of understanding the context and full scope of the alert. This is achieved by utilising threat intelligence, expanding searches within the tooling, and threat hunting for further signs of compromise. Some aspects of these steps can be automated depending on the type of alert and the Customers authority to act.

As the incident then progresses through the incident lifecycle, the following phases look to enact containment and eradication actions, which are driven in line with agreed response actions with the Customer and follow playbooks unique to each incident type (for example, Malware, DDOS, Insider Threat, Third Party Compromise). At this stage the analyst will consult the 'Authority to Act' which details what response actions an analyst is allowed to take, and items not permitted will then be escalated to the responsible team at the Customer or the relevant Redcentric Managed Service team.

Assuming permission is granted, the analyst or automation will perform these containment activities and where possible, eradicate the threat, whilst providing the Customer with appropriate updates. If required, the analyst can advise the Customer on safely recovering to a last known good configuration and provide reasonable lessons learned items.

14.19 MDR Governance Meetings

The Redcentric SDM will provide a monthly report, focusing on the performance of the Managed Cyber Security Operations Service against service targets.

The Redcentric SDM will hold a conference call to discuss the monthly report. The monthly call will include a discussion of the following:

- The effectiveness of the Custom Content applied and the need to fine tune or amend the Custom Content.
- Review of the Authority to Act and capture any concerns or issues.

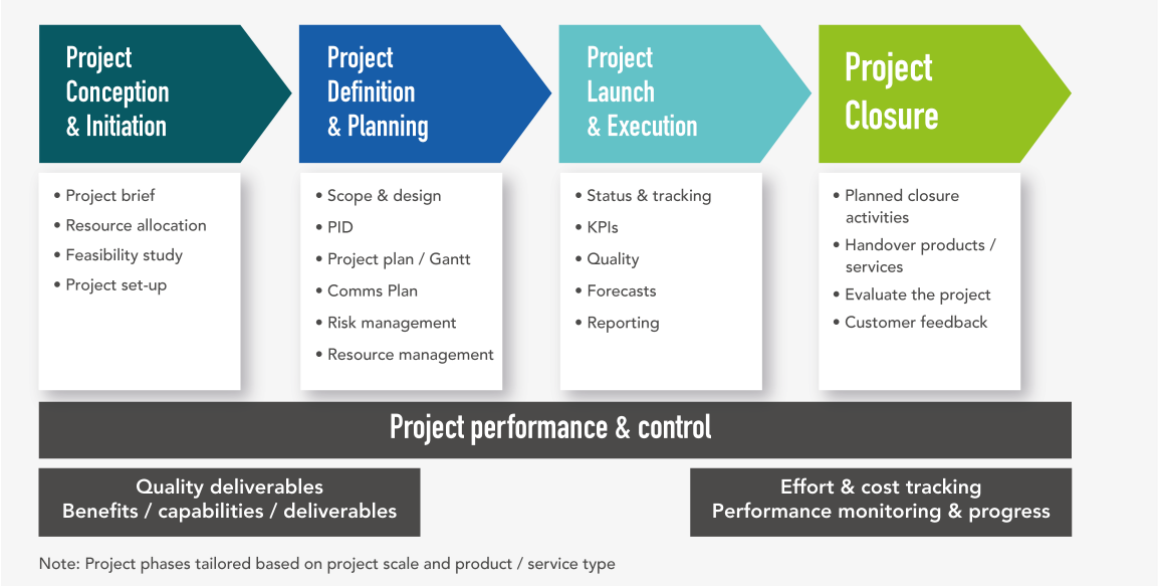
15. Project management

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 are able to promptly and effectively mitigate any challenges as early as possible.

Quality assurance processes are embedded throughout the delivery lifecycle, underpinned by our ISO 9001, 14001, 20000, 22301 and 27001 certifications and supported by our centralised programme management office.

The project toolbox

We will use a suite of project tools designed to ensure your project delivery is seamless, transparent, managed effectively, and delivered to your agreed specification. Each device has been refined over time based on our experience and as our knowledge evolves with the introduction of new technologies.

- Project initiation document to develop a detailed scope of your requirements
- Comprehensive project plan to refine the delivery approach
- High level solution design
- Low level solution design
- RAID Log to identify, control and govern project risks
- Site audit report to help identify issues and challenges at each project location

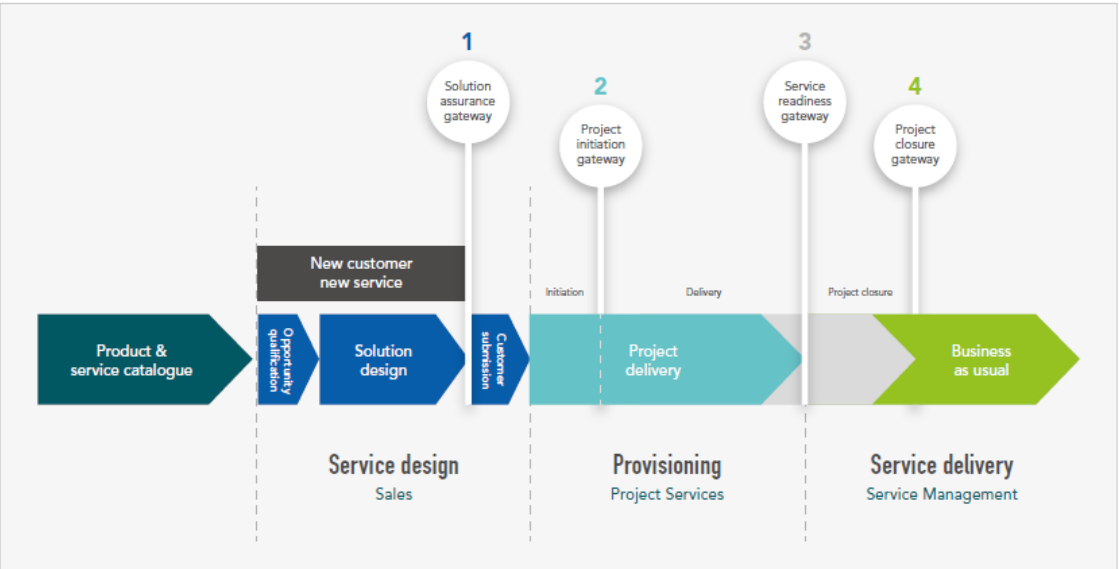
- Test plan to minimise disruption to your business operations
- Communications plan that defines what information to share and with whom
- Site implementation tracker to record the migration progress
- Weekly highlight report providing project updates
- Customer Service Pack
- UAT Test Report – per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

Transition management

It is important to Redcentric that you experience a seamless and smooth transition into your service management team. With an established and proven approach to transitioning customers from solution design, through to projects and into your support team. Redcentric are confident you will feel supported and comfortable for the project team to step back, to let the service management team take over.

Using an effective project delivery approach throughout your transition journey, will ensure:

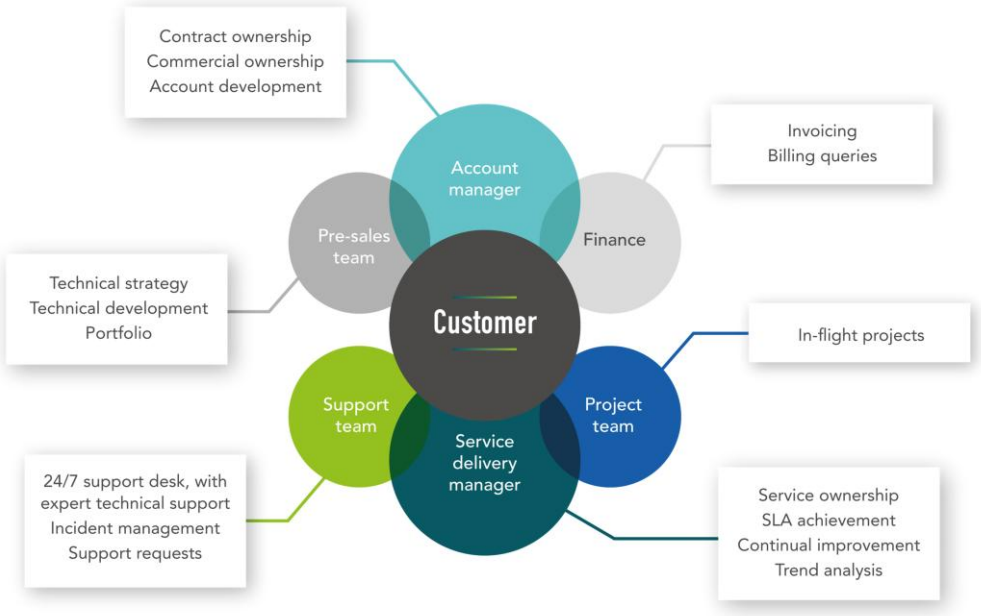
- Technical delivery is achieved on time and to specification
- The support model is fit for purpose and available at service commencement
- You will experience a 'soft landing' with minimal disruption to service.



With 30 years of track record of delivering projects, Redcentric's 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.

16. 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.

17. 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 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 subject to additional fees. As standard, we provide a service pack that includes up to 12 months of data extracted from the support system and service monitoring systems. We analyse current and previous months' performance and identify any trends.

We operate a Service Management System which meets the requirements of ISO/IEC 2000, which means we have a tried and trusted model for service delivery that provides a consistent approach.

18. 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.

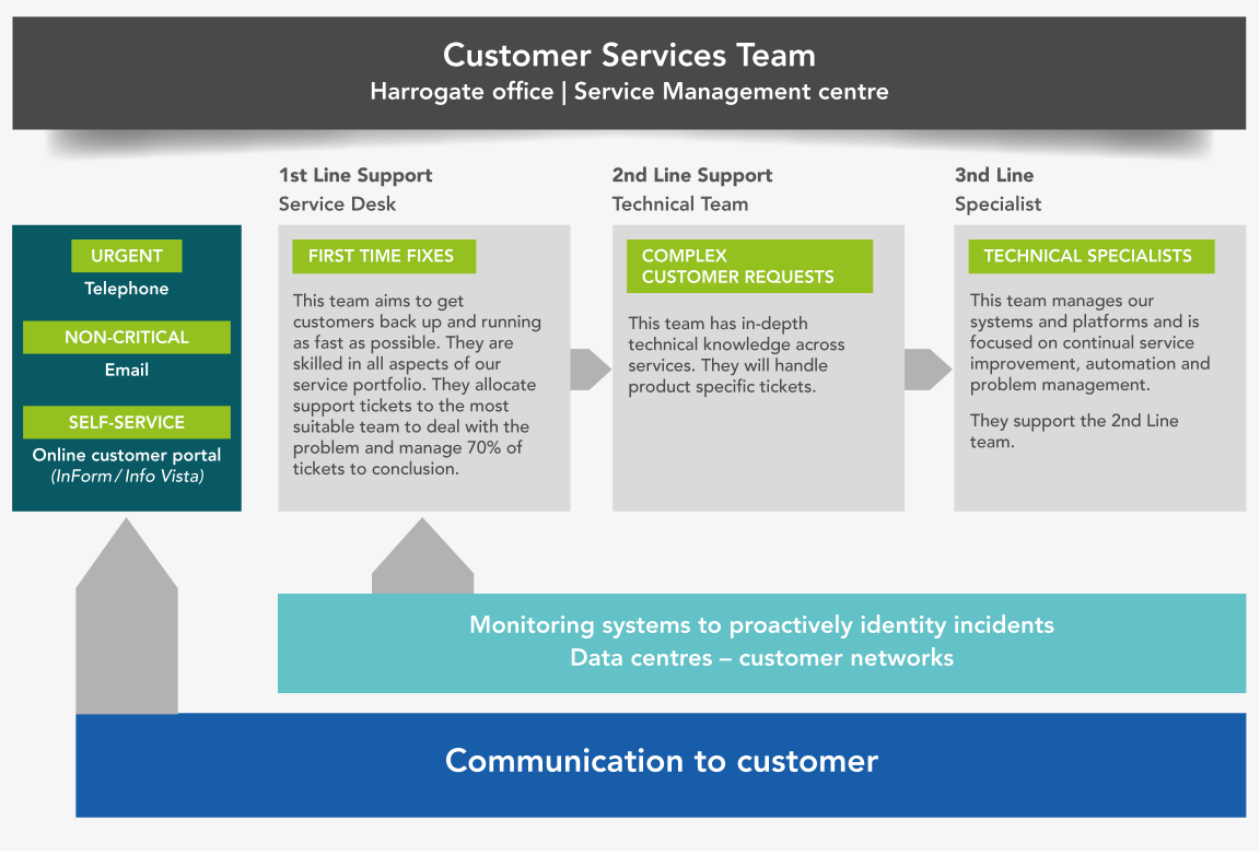
Our support operations meet the highest industry standards, and service management processes are based on the ITIL framework.

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.

19. 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.

20. 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.

21. 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.

22. 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

ISO 9001 Quality Management FS 603185
ISO 14001 Environmental Management EMS 673062
ISO/IEC 20000-1 Information Technology Service Management ITMS 658453
ISO 22301 Business Continuity Management BCMS 603184
ISO/IEC 27001 Information Security Management IS 603187