



Meraki Connectivity and Security Service Definition

G Cloud 15

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

January 2026

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1. Service Overview.....	4
1.1 Introduction	4
2. Service Description	5
2.1 Introduction	5
2.2 Related Products.....	5
2.3 Solution Design	5
2.4 Supported Appliance Types	5
2.5 Hardware ownership and licensing	6
2.6 LAN Cabling.....	7
2.7 Site Surveys.....	7
2.8 Power and Space.....	7
2.9 Deployment.....	7
2.10 Detection of Rogue Access Points and Other Security Alerts.....	7
2.11 Monitoring for Device Failure and Service Issues	8
2.12 Hardware Support	8
2.13 Access to Report Information	8
2.14 Portal Access.....	9
2.15 Meraki Portal Training	9
2.16 Wireless LAN Performance Assurances.....	9
2.17 Meraki Protection, Privacy & Security	10
2.18 Evolving Requirements	10
2.19 Public Wi-Fi Access and Communications Data.....	10
2.20 Purple - Guest Access, Location, Presence and Analytics	11
2.21 Co-management.....	11
2.22 Firmware Upgrades.....	11
2.23 Service & Responsibilities	12
2.24 SD-WAN support.....	13
2.25 License Renewal Notifications	13
3. Onboarding and Offboarding.....	14
3.1 Onboarding	14
3.2 Acceptance Criteria.....	14
3.3 Offboarding	14
4. Associated Redcentric Services.....	15
5. Service Levels and Service Credits.....	16
6. Responsibilities and Accountabilities.....	18
6.1 High Level Redcentric Responsibilities	18
6.2 High Level Customer Responsibilities	18
7. Business Continuity and Disaster Recovery	19

7.1	Business Continuity.....	19
7.2	Disaster Recovery.....	20
8.	Data Processing.....	21
8.1	Data Processing Scope.....	21
8.2	Data Storage and Encryption.....	21
8.3	Data Processing Decisions	21
8.4	Sub-Processors	21
8.5	Customer Access to Data.....	21
8.6	Security Arrangements and Options.....	21
9.	Exit Plan.....	22
10.	Project management.....	23
11.	Account management	25
12.	Service management	26
13.	Support Services	27
14.	Information assurance	28
15.	Professional services	29
16.	Company profile	30

1. Service Overview

1.1 Introduction

Meraki's range of connectivity and security devices are popular due to the market leading traffic visibility and diagnostic capabilities, also the scalability and ease of management using the cloud-based management portal. The Redcentric Meraki Service provides the design, deployment and ongoing support of Meraki's connectivity and security devices to deliver a multitude of network solutions including traditional and software-defined wide-area networks (SD-WAN) and distributed and complex wired and wireless local area networks (LANs).

2. Service Description

2.1 Introduction

Meraki's cloud managed networking devices enable customers with even modest IT support departments to provide a first-class service to their end-users. Redcentric provides design and integration consultancy to ensure the most appropriate Meraki devices are selected and integrated with other services to meet specific Customer needs. Redcentric pre-configures the cloud management platform ready for device deployment. Redcentric engineers deploy and connect the Meraki devices at Customer locations and provide end-to-end testing. Redcentric monitors the Meraki network devices and works with the Customer's IT department to identify and replace any unit that develops a fault. Further Redcentric provides a level of configuration support should the Customer require it.

2.2 Related Products

Redcentric offers an extensive portfolio of services designed to meet the requirements of companies of all sizes. Customers can focus on their core business applications when the Meraki Service is taken in conjunction with other services from Redcentric connectivity, infrastructure and unified communications portfolios. Section 2.20 details a complimentary service which, as well as providing detailed insight into the userbase, addresses the compliance obligations associated with offering a public Wi-Fi service.

2.3 Solution Design

Redcentric consultants work with the Customer to establish and document specific design objectives and requirements. The consultants then use this as the basis to produce a high-level design. The design work should include all aspects including for example Security, WAN, LAN & RF coverage where applicable.

2.4 Supported Appliance Types

Redcentric supports Meraki's current range of security, LAN switching and wireless access point devices.

Meraki MR

The Meraki MR series is the world's first enterprise-grade range of cloud-managed WLAN access points. Designed for demanding enterprise environments, the current range of MR devices deliver lower-cost Wi-Fi 5 and ultimate performance Wi-Fi 6 capability. The latter supporting high user density using MU-MIMO, special re-use and the latest modulation technologies to deliver the throughput and reliable coverage required by demanding business applications. The MR series comes equipped with industry-leading features that make them ideal for demanding enterprise deployments:

- 802.11ac and 802.11ax technologies with multiple spatial streams, built for voice and video
- Integrated enterprise security and guest access
- Dedicated radio for security and RF optimization with integrated spectrum analysis
- Integrated intrusion detection and prevention system (WIDS/WIPS)
- Self-learning application-aware traffic analytics engine
- Flexible group policy engine for creating and applying application- aware policies by network, device-type, and end-user

Meraki MS

The Cisco Meraki MS wired switch series brings the benefits of the cloud management to networks of all sizes: simplified management, reduced complexity, network wide visibility and control, with lower operational cost for campus and branch LAN deployments. Cisco Meraki access switching is available in both Layer 2 and powerful Layer 3 models. Mission-critical features like Layer 7 application visibility, network topology visualisation, virtual stacking, QoS for business-critical applications, 802.1X access control, and more — are present in all models.

Meraki MX

Built on Cisco Meraki's award-winning cloud-managed architecture, the MX is Cisco's 100% cloud-managed Unified Threat Management appliance. MX appliances self-provision, automatically pulling policies and configuration settings from the cloud. Powerful remote management tools provide network-wide visibility and control and enable administration without the need for on-site networking expertise.

Cisco Meraki MX Security Appliances are ideal for organizations with large numbers of distributed sites. Since the MX is 100% cloud managed, installation and remote management is simple. The MX has a comprehensive suite of network services, eliminating the need for multiple appliances. These services include Layer 7 application firewall, content filtering, web search filtering, intrusion prevention, web caching, Intelligent WAN with multiple uplinks.

Cloud services deliver seamless firmware and security signature updates, automatically establish site-to-site VPN tunnels, and provide 24x7 network monitoring. Moreover, the MX's intuitive browser-based management interface removes the need for expensive and time-consuming training.

The MX platform has an extensive suite of security features including IPS, content filtering, web search filtering, antivirus / anti-phishing, geo-IP based firewalling and IPsec VPN connectivity, while providing the performance required for modern, bandwidth-intensive networks.

Layer 7 fingerprinting technology lets administrators identify unwanted content and applications and prevent recreational apps like BitTorrent from wasting precious bandwidth.

The platform delivers superior intrusion prevention coverage, a key requirement for PCI 3.0 compliance. The MX also uses the Webroot BrightCloud® URL categorization database for CIPA / IWF compliant content- filtering, Kaspersky Safestream II® engine for anti-virus / anti-phishing, and MaxMind for geo-IP based security rules.

Best of all, these industry-leading Layer 7 security engines and signatures are always kept up to date via the cloud, simplifying network security management and providing peace of mind to IT administrators.

Meraki vMX

vMX virtual appliances can extend a customer software defined wide area network (SD-WAN) to include their third-party hyperscale cloud environments. Redcentric supports Meraki vMX virtual appliances deployed by the customer within the customer third-party hyperscale cloud environment subscription.

2.5 Hardware ownership and licensing

All Meraki products require licensing to operate. Meraki's licensing combines ongoing software upgrades with centralised systems management and hardware support. Meraki operates two license models: co-termination and per device. When co-termination licensing is implemented and additional devices are added to the Customer's inventory during the license period, the license expiration date for all devices is adjusted such that the existing and new devices expire together. When per-device

licensing is implemented and additional devices are added to the Customer's inventory during the license period, the license expiration date of existing devices does not change – commonly resulting in device licenses expiring at different times.

Redcentric offers two options, 1) an overlay service where the Customer owns the hardware and is responsible for the purchase of licenses and 2) where Redcentric supplies the hardware and licensing as part of the service. When the customer wishes to own the Meraki hardware, they are also responsible for the purchase of ongoing operation licences. As a Meraki re-seller, Redcentric is well-placed to supply hardware and licensing on a sale basis.

If the Customer wishes to own the Meraki hardware, it is the Customer's responsibility to buy, renew and/or extend licenses when required to keep the environment operational. If there is an infringement or when licenses lapse, the Meraki cloud management platform will ultimately stop devices passing traffic. Please consult Meraki's website for up-to-date details of this critically important aspect.

2.6 LAN Cabling

The Redcentric Meraki service does not include any structured cabling checks, cable work or patching between the Customer's existing wired switch infrastructure and the location of each Meraki device. Redcentric will undertake a general or detailed survey of existing structured cabling on request and provide a report on its suitability. Redcentric can arrange for cabling to be upgraded, repaired, corrected, extended, tidied, re-patched, labelled and replaced as required to ensure a customer's entire LAN is fit for purpose. This work is chargeable.

2.7 Site Surveys

Customers can select optional site surveys which generally results in a design more likely to meet specific requirements. This is particularly applicable when aged LAN wiring exists and when Meraki Access Points are to be deployed and wireless coverage is critical.

2.8 Power and Space

The Customer is required to provide space in a suitable environment at each site for the various pieces of equipment required to deliver the service. In addition, the Customer is required to provide sufficient suitable 13A mains power points within 1m of the various pieces of CPE. Note that in some cases, LAN switches can provide power to Access Points using power-over-Ethernet.

2.9 Deployment

Redcentric generally undertakes physical installation, configuration, commissioning, and testing of the Meraki Access Points, switches and security devices which form part of the agreed design. Project management and engineering charges apply to cover this work.

Where vMX software appliances are required as part of a design, the Customer is required to undertake deployment in their subscription within 3rd -party hyperscale cloud environments.

The Redcentric commercial offer is based on the premise that site access will be available between 9am and 5pm Monday to Friday and on-site work will be undertaken during this time unless specifically agreed in writing.

2.10 Detection of Rogue Access Points and Other Security Alerts

Meraki's cloud managed wireless access points (APs) come equipped with Air Marshal, a built-in wireless intrusion detection and prevention system (WIDS/WIPS) for threat detection and attack remediation. APs configured in Air Marshal mode will scan their environment in real-time and take pre-emptive action based on intuitive user-defined preferences. Air Marshal triggers alarms and can be configured to automatically contain suspect and known rogue APs. Intuitive cloud-based

management with flexible remediation policies makes Air Marshal ideal for security conscious distributed networks.

The Customer is solely responsible for monitoring, investigating, and eliminating rogue access points and investigating other security alerts.

2.11 Monitoring for Device Failure and Service Issues

Redcentric systems poll the cloud management platform approximately every 5 minutes to confirm that each Meraki device is available. This is in line with industry standard network management best practices. If a device does not respond to several successive polls, an automatic alert is forwarded to the Redcentric network fault management system.

Section 2.23 details two service options. When the Customer selects the Managed option, the system also monitors for sustained delay and packet-loss on WAN links and automatically raises alerts accordingly.

Alerts result in the automatic generation of an incident which is placed in the technical support queue. Technical support engineers investigate these incidents 24 hours a day, 365 days a year.

Customers can become aware of problems in the short window before the polling procedures verify a problem and issue an alert. Redcentric provides additional means for Customers to raise faults, i.e., via telephone, email, and the web portal.

Redcentric classifies problems according to severity. This allows the prioritisation of resource on issues that have the most impact on Customers' businesses. Further details of the classifications can be found in the Redcentric Customer Welcome Pack which is available on request.

Redcentric is committed to continually improving and expanding its services, and to facilitate these improvements, it is necessary to carry out essential work from time to time. In accordance with Information Technology Infrastructure Library (ITIL) service management standards, these activities are carefully scheduled using an internal change control process; this gives Customers maximum visibility of any given change and thereby ensures that planning and implementation is carried out to minimise the effect on Customers using Redcentric services.

Maintenance windows and procedures for communicating emergency outages are detailed in the Customer Welcome Pack.

2.12 Hardware Support

If Redcentric support desk staff, in conjunction with the Customer and Meraki support staff, determine that a piece of Meraki equipment has developed a fault, Redcentric will work with Meraki to have a replacement unit shipped. Meraki usually aim to despatch hardware replacements within 24 hours of accepting a valid RMA request. Customers wishing to minimise down-time resulting from hardware failure are advised to buy spare devices and store them at their location(s) for immediate replacement or incorporate spare active devices into the design – i.e., high-availability design. To minimise expense, the Customer is required to perform the straightforward operation of swapping faulty units under instruction from Redcentric staff if required. The Customer is also required to return faulty units. Enhanced support options including on-site engineering assistance are available to meet specific Customer requirements and must be agreed in writing by both parties prior to finalising a Service Agreement.

2.13 Access to Report Information

The Meraki cloud-based management platform provides extensive information on all aspects of the environment. The Customer will be able to access this information directly through the portal and

configure and modify reports as required. Therefore, Redcentric does not create or modify or issue reports etc. but will happily assist the Customer if required.

2.14 Portal Access

The Customer's administrative staff will have full read access on the Meraki portal as well as write access so that they can make changes to certain aspects of the Meraki platform as detailed below.

Redcentric Staff will have unrestricted access to the Meraki portal to provide support to the Customer.

There are two basic types of Dashboard administrators: Organisation and Network.

Organization administrators have complete access to their organisation and all its networks. This type of account is equivalent to a root or domain admin, so it is important to carefully maintain who has this level of control. Please see below for best practices regarding these accounts.

Network administrators have access to individual networks and their devices. These users can have complete or limited control over their network configuration, but do not have access to organization-level information (licensing, device inventory, etc).

Most Dashboard administrators will fall into one of the two above categories, the information below details the options and limitations associated with different admin types.

Organisation Permission Types

Read-only: User able to access most aspects of network and organization-wide settings, but unable to make any changes.

Full: User has full administrative access to all networks and organization-wide settings. This is the highest level of access available.

Network Permission Types

Guest ambassador: User only able to see the list of Meraki authentication users, add users, updated existing users, and authorize/de-authorize users on an SSID or Client VPN. Ambassadors can also remove wireless users if they are an ambassador on all networks.

Presented with user management portal only.

Monitor-only: User only able to view a subset of the Monitor section in Dashboard and no changes can be made.

Read-only: User able to access most aspects of a network, including the Configure section, but no changes can be made.

Full: User has access to view all aspects of a network and make any changes to it.

2.15 Meraki Portal Training

The Cisco Meraki portal has been developed over time to be both highly functional and intuitive. Meraki have an extensive range of self-paced, easy to access training videos available on YouTube® covering a wide range of functions to assist network administrators. Further, classroom training courses are available which underpin a formal certification programme if required. Portal training is therefore not provided as part of the Meraki Service.

2.16 Wireless LAN Performance Assurances

Due to the nature of wireless networks where environmental conditions change constantly and it is not possible to control user density, any issues relating to RF interference and bandwidth congestion are beyond Redcentric's control, (e.g., coverage, throughput, bandwidth availability etc.).

Redcentric will on-request undertake on-site investigation and site-surveys to identify issues, which may for example result in a recommendation to install additional access points. Investigation and remediation work is chargeable.

2.17 Meraki Protection, Privacy & Security

Cisco Meraki is committed to data protection, privacy, and security and has designed its cloud architecture specifically in a way that enables customers to securely protect their data. European customers can confidently deploy scalable, secure Meraki networks that comply with applicable data protection regulations across the European Economic Area (EEA).

The Meraki EU Cloud

The Meraki cloud architecture leverages a globally distributed public cloud architecture that provides built-in reliability, security, and redundancy. To meet the needs of European customers, Meraki created the EU Cloud, a separate part of the Meraki cloud architecture designed to meet the needs of European customers and regulations. Hosted on data centres located exclusively in the EEA, the Meraki EU Cloud provides reliability and business redundancy offered by a distributed architecture while ensuring that no personal data leaves the EEA.

Additionally, the EU Cloud's out-of-band architecture ensures only management information, and not network traffic, passes through EU Cloud datacentres. The EU Cloud architecture enables customers to satisfy their legal obligations and simultaneously realize all the advantages cloud management offers, including centralized visibility and control, unified management of wireless and wired networks, and reduced operational expense.

The Meraki EU Cloud is built on a PCI DSS Level 1 certified system architecture and operates with a 99.99% Service Level. Additionally, Meraki EU Cloud data centres are certified with one or more of the following: ISO 9001:2008, ISO 27001:2008 & PCI DSS

Meraki and the EU Cloud are compliant with the following applicable European data protection regulatory frameworks and local laws: EU Directive 95/46/EC, German Federal Data Protection Act & Article 29 Working Party Opinion of July 1, 2012

2.18 Evolving Requirements

Redcentric is committed to delivering solutions that meet Customers' evolving needs. Consequently, when possible, Redcentric is happy to accommodate changes to the service as required during the contract period. Any changes to the service requiring design work, additional coverage, or support for new features, VLANs or WLANs etc. may incur design, hardware, software, licensing, implementation, support and/or other charges.

2.19 Public Wi-Fi Access and Communications Data

Where applicable, wired and/or wireless access to the Internet is provided to end users by the Customer, and not by Redcentric (Redcentric will provide such services to the Customer separately if ordered). The Meraki Service must be branded accordingly in communications to end-users.

The Customer will be responsible for all user management in relation to the Services, including (1) (unless otherwise agreed in writing) user authentication and (2) maintaining and supplying to government agencies etc. any records relating to the use of the Service as required by law from time to time.

Please see section 2.20 detailing Redcentric's complementary service intended to reduce administrative burden and mitigate risk associated with offering these services to end users.

2.20 Purple - Guest Access, Location, Presence and Analytics

The Purple cloud-based service delivers a guest Wi-Fi capability that benefits all parties. Users' login easily using a variety of methods including social media for fast, effortless access.

The portal pulls together multiple data sources allowing businesses to see real-time footfall, passers-by, conversion and bounce rates, dwell times, return visits and frequency; enabling businesses to truly understand their venues. Businesses can then act when people are in venue using marketing tools to target users through email, SMS and customisable splash pages.

Using Wi-Fi, Bluetooth and GPS, the system can enable additional location services to pinpoint Customer movement in venues down to a few metres. Businesses can then send hyperlocal marketing messages to people as they move around the venue in real-time.

The system has a restful API, so the data displayed in the Portal can be connected to the Customer's other information systems such as CRM and ERP.

The Purple service has proven integration with Meraki infrastructure.

The Purple service can be configured for content filtering. By using the service, the end-user enters into an agreement with Purple. Consequently, the service is provided to end-users by Purple, and not the Customer. Requests for legal intercept and Regulation of Investigatory Powers Act (RIPA) enquiries are handled by Purple.

2.21 Co-management

The Customer's administration staff can make changes to the Meraki environment via the cloud-based management portal. This approach benefits both parties as it removes some administration burden from Redcentric, and the Customer can implement trivial changes very quickly and provide support to end-users (e.g. Search for failed authentication events). However, these co-managed arrangements can pose problems. If Redcentric determines, at its sole discretion, that changes implemented by the Customer's staff have contributed to an issue which impacts Redcentric's ability to provide the service, Redcentric may charge the Customer for any remediation work.

2.22 Firmware Upgrades

Meraki release firmware upgrades from time-to-time which fix software bugs or deliver new features or functionality. Depending on the level of Management, as detailed in section 2.23, upgrades on the Customer's devices may be scheduled by the Customer or Redcentric staff. When Redcentric staff are responsible for scheduling upgrades, Redcentric will:

- Notify the Customer of the proposed upgrade date/time, giving at least 10 business-days' notice.
- Schedule upgrades Monday-Friday, 4am-7am where additional staff are present to oversee issues relating to upgrades should they occur.
- Accommodate Customer requests for postponed or alternative upgrade slots where possible

Customers are advised to specify, as part of the order, a test environment which can be used by them to test upgrades prior to roll-out across their entire estate of devices

If the firmware or hardware version of your Meraki appliance is forecast to become End of Support (EoS) / End of Life (EoL) during an initial contract term or a renewal of that contract term, Redcentric will no longer be able to provide security or critical firmware updates for that EoS or EoL Appliance.

To continue to receive security and critical updates, a hardware refresh of the specific Meraki Appliance will be required. Any hardware refresh, including the provision of new Meraki Appliance, is outside the scope of this Service and will be chargeable. A new Meraki Appliance would be provided by Redcentric for an additional charge.

2.23 Service & Responsibilities

Two on-going support models are available to meet the needs of Customers requiring different levels of control.

In addition to other responsibilities detailed in this definition, a list of typical tasks is shown in the table below with details of responsibility for the two service options.

Function	Monitored	Managed
Routine low-level changes LAN. e.g. port speed, VLAN allocation etc.	Customer	Redcentric
Routine low-level changes Security. e.g. change to rule-base, content filters etc.	Customer	Redcentric

Function	Monitored	Managed
User database administration	Customer	Redcentric
Schedule firmware updates	Customer	Redcentric
Reaction to failed or degraded links when delivering SD-WAN functionality	Customer	Redcentric

In addition to responsibilities in the table above, Redcentric is responsible for the following regardless of which option is chosen:

- Initial configuration, deployment, and testing of the overall solution
- Periodic polling of devices to detect failure
- Coordinating replacement of faulty hardware
- Templated changes effecting critical elements / whole network - e.g. routing
- Deployment of Customer purchased device licenses on Meraki cloud controller if supplied by Redcentric
- Deployment of device licenses on Meraki cloud controller (License Included option)

In addition to responsibilities in the table above, the Customer is responsible for the following:

- Providing Redcentric with the technical details required for the design. E.g., WLAN IP address ranges, SSID names, VLAN assignments, local DNS servers, DHCP scopes and options etc.
- Provision of suitable power, space, and cabling
- Configuring and accessing reports as required
- Meeting any compliance requirements associated with offering a public Internet service to guests (the Customer may choose to use Redcentric's Guest Management, Analytics and Marketing service to achieve this)
- Monitor and address rogue AP & other security aspects
- Procuring Meraki device operational licenses as required. (Customer owned hardware & License option)
- Deployment of device licences on Meraki cloud controller if not supplied by Redcentric (Customer owned hardware & License option)
- Test upgrades prior to roll-out across their entire estate of devices
- Where applicable, diagnose end-user issues and provide support

2.24 SD-WAN support

Meraki MX and vMX devices can deliver SD-WAN functionality. This allows Customers to build a WAN from a mix of private (e.g., MPLS) and public (i.e., Internet) connections from multiple suppliers using a variety of transport technologies (e.g., Broadband, Ethernet & cellular).

The Meraki devices route the Customer's application traffic according to the policy configured on the Meraki cloud controller. Traffic can be encrypted over private links as well as public (i.e., Internet) links. Thresholds for delay, jitter and packet-loss can be set 'per application'. The system measures these parameters and routes application traffic accordingly. If desirable, the system can be configured to share application traffic across multiple links. For sites that have a link to the Internet (i.e., a direct Internet access [DIA] circuit), the system can be configured to provide local break-out. This is optimal for traffic destined for public Internet facing applications (e.g., applications hosted in Azure or AWS). Providing local break-out also frees up valuable bandwidth on private links that would otherwise be used to carry the traffic to a central breakout point.

When the Customer chooses to take the Managed Service (see section 2.23), Redcentric monitoring systems poll the devices periodically to identify link failures and sustained link quality issues. Redcentric investigates issues relating to connectivity services it provides. Issues relating to third-party connectivity supplied by the Customer are reported to the Customer - Redcentric does not deal with third-party connectivity suppliers directly.

2.25 License Renewal Notifications

When license renewal approaches, Meraki emails Administrators configured on the Cloud Portal with license reminder notifications – these reminders become more frequent as the license end-date approaches. Commonly both Redcentric and Customer staff are configured on the portal so both parties receive these notifications. Customers that have elected to own the Meraki Hardware, and therefore take responsibility for licensing, should contact their Redcentric account manager to discuss timely purchase of renewal licenses and renewal of the Redcentric overlay Page 10 service. Where Redcentric retains ownership of the hardware, Redcentric will renew the licensing after the Customer has signed a contract renewal/extension for the Redcentric service.

3. Onboarding and Offboarding

3.1 Onboarding

Redcentric offer a fully managed service with advice and guidance based on customer requirements for resiliency, cost, throughput capability requirements. We design solutions based on customer supplied floor plans, building infrastructure information and other factors to determine the best solution for each site environment.

Our project and delivery teams fully implement the service, including configuration and testing, and work closely with customers to ensure the delivery of services to the required specifications.

3.2 Acceptance Criteria

Criteria listed below apply to the Meraki Service:

- All Meraki devices appear on the cloud management portal
- A sample of wired or wireless devices can connect to the network (after authentication when implemented)
- The Customer can access cloud management administration portal

3.3 Offboarding

Redcentric project, delivery and support teams will work closely with customers to gracefully closedown any services at their contract end and, if required, assist in any transition or migratory tasks with the customer and any new service provider.

Redcentric will not be obliged to disclose any confidential information to the customer or replacement supplier, or to transfer any assets, contracts, employees, or third-party licences.

3.4 Principles

Redcentric will assist the customer in facilitating the orderly transition of the services (in whole or part) from Redcentric to the customer or any replacement supplier upon the expiry or earlier termination of the Order Form for Access as a Service.

3.5 Removal of Customer Premises Equipment

“Customer Premise Equipment (CPE)” is defined in paragraph 1.6 of this Service Definition. On termination or expiry of the Call-Off Contract, the customer must undertake the following responsibilities:

- agree a time and date for the CPE to be removed by Redcentric; and then
- permit Redcentric to remove the CPE at the agreed time on the agreed date in a sequence to be specified by the customer.

3.6 Additional Transition Assistance

Where the customer requests the provision of additional transitional assistance, in addition to that required under this section, Redcentric shall provide such assistance as additional Professional Services upon agreement and signature of a Variation Order. The additional transitional assistance detailed here shall be chargeable at the Redcentric prevailing time and materials consultancy day rates.

4. Associated Redcentric Services

The table below provide details of other compatible services with Meraki Connectivity and Security available from Redcentric via G-Cloud 15.

Service Name	Service Summary
Network as a Service	Network as a Service provides a secure internal / external network connection. It meets compliance standards and various Redcentric services such as internet and security can be overlayed over this single connection into the Redcentric Network.
DDOS Mitigation Service	DDoS Mitigation Service consists of three services. DDoS Essentials and DDoS Essentials Plus, ensures customer protection within 60 or 15 minutes respectively, upon attack notification. DDoS Pro offers comprehensive management with instant detection and automated response. Monitoring at the ISP level enables pro-active attack identification, enhancing network security measures.
Managed Firewall Service	Managed Firewall Service The service is delivered on virtual firewalls on a shared platform or on one or more dedicated hardware firewall appliances. The firewalls control traffic between devices on different networks and provide perimeter protection. The firewall is configured by our staff to meet customer's requirements. Firewalls are monitored for alerts.
Managed LAN Switch Services	Managed Local Area Network (LAN) Switch Services provides an Ethernet LAN switch located on a customer site to provide connectivity between compatible, hard-wired Ethernet LAN devices. Typically, the switch would be the central connectivity point for PCs, Internet Protocol (IP) phones, servers, printers etc.
Managed SD WAN Service	Managed SD WAN Service is designed to complement traditional private IP-VPN networks. It allows customers to make optimum use of the available bandwidth at sites, and to supplement private connections with cellular, low-cost Internet and other links. Application visibility, control and performance can be enhanced, delivering greater efficiency and user satisfaction.
Managed Wireless LAN Service	Managed Wireless LAN Service offers design, deployment, monitoring, support, and management of wireless LAN infrastructure deployed on Customer sites. The service uses products from leading Wireless LAN manufacturers. The service delivers enterprise features and uses local or cloud-based systems for provisioning, monitoring, and management.
Secure Remote Access Service	Secure Remote Access Service offers a robust, scalable, flexible, and secure way for remote users to access information and business applications whilst away from their usual work location. Software on the user's device communicates with the remote access platform across any Internet connection and a secure tunnel is established.
Two Factor Authentication	Two Factor Authentication (2FA) service offers a robust, flexible, and secure way to authenticate user connection requests to network devices. The 2FA service can be deployed on both Customer managed and Redcentric managed network devices. The 2FA service offers a more secure and scalable alternative to static passwords.
Wireless Guest Access	Wireless Guest Access is an analytics and marketing service provided by our partners Purple. Redcentric resells, integrates, and supports the service. Used with wireless services to provide guest Wi-Fi experience, and venue owners valuable information on their customers and visitors, focused marketing communication and assists in the compliance implications associated.

5. Service Levels and Service Credits

5.1 Service Levels

The Service Level applicable to the Meraki Service is as follows:

Service Level:	Service Availability:
Availability of each individual Meraki Device	Not less than 99.5%

5.2 Exclusions from Availability

In calculating Availability, in addition to the exclusions listed in clause 7.9 Part A - General Terms of the Redcentric G Cloud 15 Supplier Terms the following shall be excluded where it is proven or suspected beyond reasonable doubt:

- Failure of any element not supplied by Redcentric which prevents Redcentric from measuring Availability
- Unavailability due to throughput (load) exceeding initial documented requirements
- Unavailability due to onsite power, cabling, or local network issues
- Malicious attempts to disrupt service such as wireless jamming, Denial of Service etc.
- Any impact caused in-whole or in-part by configuration changes made by the Customer
- Suspension of the Service by Meraki due to licensing violation (Customer Supplied option)
- Suspension of the Service by Meraki due to licensing violation caused by the Customer (License Included option)
- Impact caused by Meraki software/firmware upgrade regardless of whether it was evaluated on test equipment prior to roll-out
- Unavailability due to hardware failure when non resilient design is implemented
- Unavailability of vMX software located in 3rd-party cloud environments for any reason other than misconfiguration by Redcentric staff

5.3 Floor Service Level

The Floor Service Level applicable to the Meraki Service in respect of Availability shall be 85% per device in any given month, i.e., each device has its own Availability Service Level and its own Floor Service Level.

5.4 Service Credits

The Service Credits applicable to the Meraki Service shall be calculated as follows:

For each device where availability is < 99.5% in the relevant Month, a Service Credit may be claimed according to the table below. For the avoidance of doubt, for the purposes of paragraph 6.4 of the General Terms, the maximum value of Service Credits in any Month shall be a sum equal to half the Charges which would have been payable in respect of the aggregate of all Meraki Service devices in that Month had Redcentric provided the Meraki Service in accordance with the applicable Service Levels.

In the following table: “≥” means “greater than or equal to” and “<” means “less than” “MS” means the average Charge payable for an Access Point in respect of the Meraki Service for the same month

Service Availability	Service Credit
≥ 99.5%	None
≥ 99.0% but <99.5%	5% of MS

Service Availability	Service Credit
≥ 96.5% but < 99.0%	15% of MS
< 96.5%	20% of MS

6. Responsibilities and Accountabilities

6.1 High Level Redcentric Responsibilities

Redcentric is responsible for the following aspects:

- Solution design based on information and requirements provided by the customer
- Initial installation and testing of equipment with agreed success criteria
- Configuration of the centralised management, reporting, etc. components
- General upkeep of the service including hardware and software upgrades
- Ongoing support of customer-specific configuration, including advice and implementation of minor changes
- Continued monitoring of equipment with our support teams and pro-active management of faults
- Arranging replacement of faulty hardware

6.2 High Level Customer Responsibilities

The Customer is responsible for all other aspects including, but not limited to:

- Providing Redcentric with the Customer's detailed functional and other requirements
- Providing Redcentric with the technical details required for the design. E.g. Firewall rulesets, Port speeds/duplexes, uplink/downlink specifications to other equipment, IP address ranges, VLAN assignments, local DNS servers, DHCP scopes and options, NAT translations, SSID names, etc.
- Where equipment is to be located at customer premises, providing an appropriately physically secured location to house equipment, typically a communications rack in a separate communications room, or similar
- Where equipment is to be located at customer premises, providing appropriate power, rack space and heating/ventilation/cooling (HVAC) for any equipment housed on the customer's site
- Where equipment is to be located at customer premises, unless otherwise agreed with the customer, providing appropriate LAN side cabling, cables, patch panels, etc beyond the service demarcation point, unless a Redcentric managed LAN service is taken
- Where equipment is to be located at customer premises, arranging and allowing access to site facilities at agreed times and for an appropriate window of time for the installation of any equipment related to the delivery of the service
- Where equipment is to be located at customer premises, completion of any required site risk assessment information prior to engineer site visits
- Supply and upkeep of staff entitled to request changes with our support teams
- Completion of appropriate forms to request any changes to firewall rulesets, policies, etc

7. Business Continuity and Disaster Recovery

7.1 Business Continuity

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

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

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

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

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

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

Testing

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

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

Network resilience

Our network is designed and engineered to deliver highly available, stable connectivity to maintain business access to critical applications. To maximise resilience, multiple carriers provide core connectivity and routing, and switching devices are from market leaders Cisco Systems. The network design and build are geographically resilient providing a minimum of 99.99% availability (to resilient end points).

The Redcentric highly resilient, high-capacity core has connections to several carriers providing multiple options for our internal business operations and critical services, and customers wishing to access cloud services, applications, and data:

- Geographically resilient connectivity to multiple Tier-1 Internet transit providers and Internet exchanges.
- Geographically resilient connectivity directly into the inner core of the HSCN network.
- Core network engineered to withstand multiple concurrent failures and to re-route around a failed transit path in under a second.

7.2 Disaster Recovery

Management platforms are multiply resilient across geographically diverse locations and thus disaster recovery is automatically built into the service, however, the management platforms do not, in and of themselves, limit the functionality of the service. In the event that management platforms become unreachable, the immediate functionality of the service is not affected.

In terms of deployed equipment, we recommend that customers take a pragmatic approach to the deployment of access points, switches and firewalls in any location and recommend that any deployment includes additional equipment to provide resiliency in the event that a single device becomes unserviceable. In the event of service failure, our support teams work closely with the customer to replace supported equipment in a timely manner.

8. Data Processing

8.1 Data Processing Scope

- The Redcentric Meraki Service delivers design, deployment, and support functions.
- The Redcentric Meraki Service does not involve any storage or backing up of data.
- The Customer must separately enter into an agreement with Meraki, a division of Cisco Systems to use the hardware and cloud-based management portal.

8.2 Data Storage and Encryption

- Redcentric configures equipment to encrypt traffic according to Customer requirements.
- Redcentric does not capture, inspect, analyse, store, or share the Customer's traffic/data under normal circumstances.
- Under certain circumstances, when managing a support ticket, Redcentric may capture, inspect, analyse and/or store a small sample of the Customer's traffic to investigate and diagnose a very specific problem, e.g., to help resolve a problem relating to packet corruption. Such diagnosis would involve the examination of a small sample of packets, and this will only be undertaken at the request of and in conjunction with the Customer.

8.3 Data Processing Decisions

- Redcentric does not make any data processing decisions in relation to the Meraki Service. Any processing of data over Customer systems when using the Meraki Service for transit is instigated, configured, and managed by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Meraki Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

8.4 Sub-Processors

Except for physical deployment, no third parties are involved in delivering the Meraki Service, and there are no sub-processors appointed by Redcentric.

The Customer must separately enter into an agreement with Meraki, a division of Cisco Systems, to use the hardware and cloud-based management portal (and to avoid doubt, Meraki is not a sub-processor of Redcentric for this purpose).

8.5 Customer Access to Data

The Customer control its own platforms which use the Meraki Service to carry data, and the Customer therefore has full access to its own data.

8.6 Security Arrangements and Options

Meraki devices are located at Customer locations/sites. It is the Customer's responsibility to ensure physical security at such locations/sites meets its needs.

9. Exit Plan

Upon expiration of the Contract where the customer chooses not to renew with Redcentric, the steps set out in paragraph 3.3 will apply.

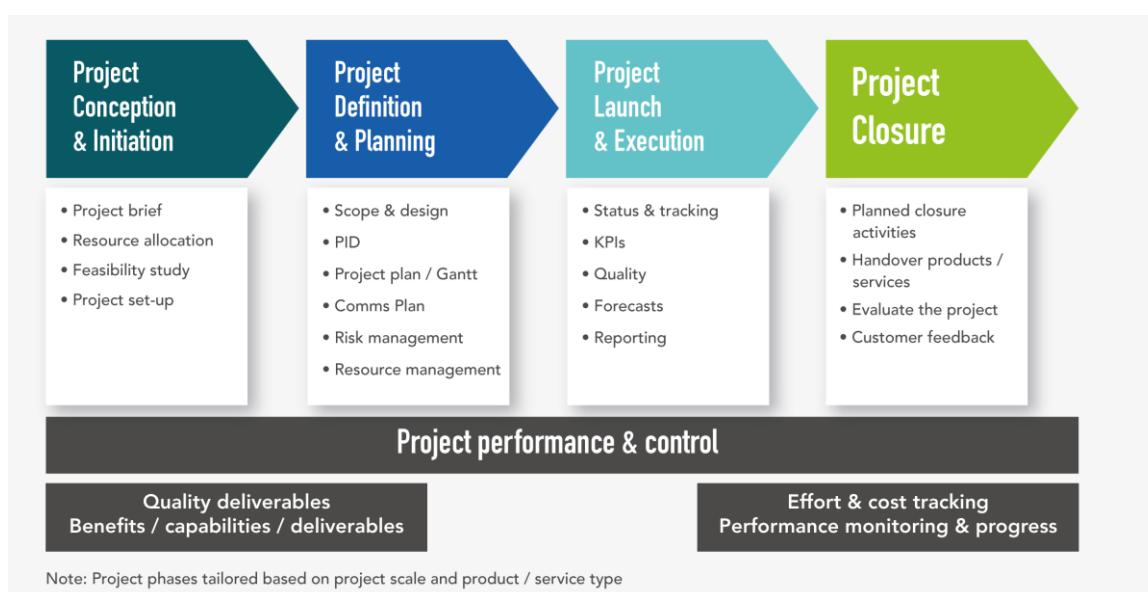
10. Project management

We understand you need to be confident we can deliver projects successfully and without risk to you or your customers. We know collaboration and communication with you is the key to successful project delivery, and the best way to ensure we can deliver the business value you expect from us.

Redcentric uses a hybrid project approach based on PRINCE2 and Waterfall methodologies, that is strengthened by ITIL project best practise. Our approach has been honed to foster a close working relationship between you and the dedicated project team that will be responsible for the onboarding of your new services.

The 4 phased approach that will steer your project delivery is:

- **Phase 1 – Conception and initiation**
- **Phase 2 – Definition and planning**
- **Phase 3 – Execution**
- **Phase 4 – Handover and closure**



We recognise the importance of making sure your project and programme of work is delivered on time and meet your quality and cost considerations. Our highly skilled team of project managers have years of project management and solutions expertise which enables us to provide you a clear understanding of when your solutions will be delivered in preparation for a seamless handover into live service.

You will benefit from our experience of managing a very broad spectrum of complex projects across our range of solutions for customers in a variety of sectors including highly sensitive sectors such as healthcare where disruption to BAU might result in a risk-to-life, or commercial sectors for example, retail or legal, where any disruption would have a significant impact on operational or commercial outcomes for the customer.

To meet your individual needs, we understand we need to be flexible to ensure we can deliver results quickly and with the expected outcome for the project. To achieve this, we will work closely with you to understand your needs and learn how issues impact your business. This will provide a clear insight into working together to resolve any challenges.

The main advantage of our meticulous approach is the handover process at each stage of the project. Risk is a key part of the agenda, which in turn promotes the continuity of risks and the identification of assumptions, issues, and dependencies. This early and continuous detection of risk means we can promptly and effectively mitigate any challenges as early as possible.

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

The project toolbox

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

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

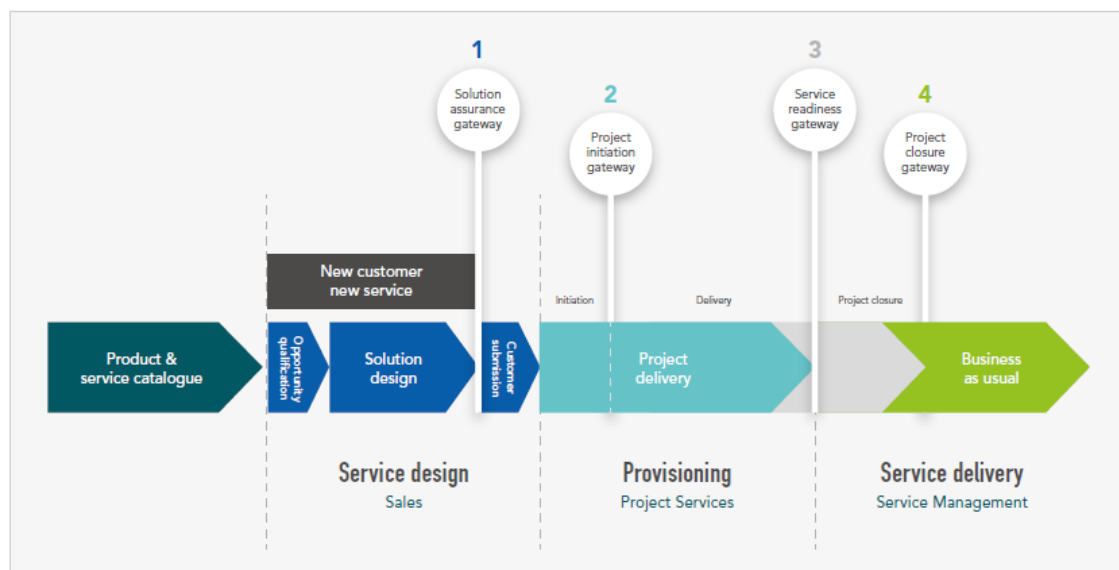
- Test plan to minimise disruption to your business operations
- Communications plan that defines what information to share and with whom
- Site implementation tracker to record the migration progress
- Weekly highlight report providing project updates
- Customer Service Pack
- UAT Test Report – per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

Transition management

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

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

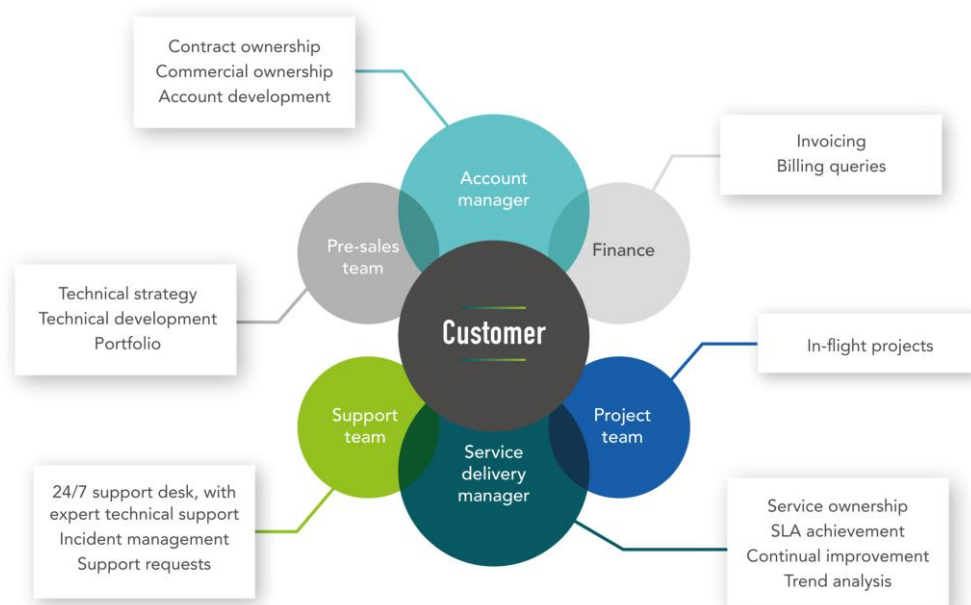
- Technical delivery is achieved on time and to specification
- The support model is fit for purpose and available at service commencement
- You will experience a 'soft landing' with minimal disruption to service.



With 30 years of track record of delivering projects, Redcentric is knowledge and approach to mitigating risk during the project transition phase is based on experience. Their mature and proven approach is employed as a standard risk management framework which flows from initial bid stage through to project delivery, and into live service.

11. Account management

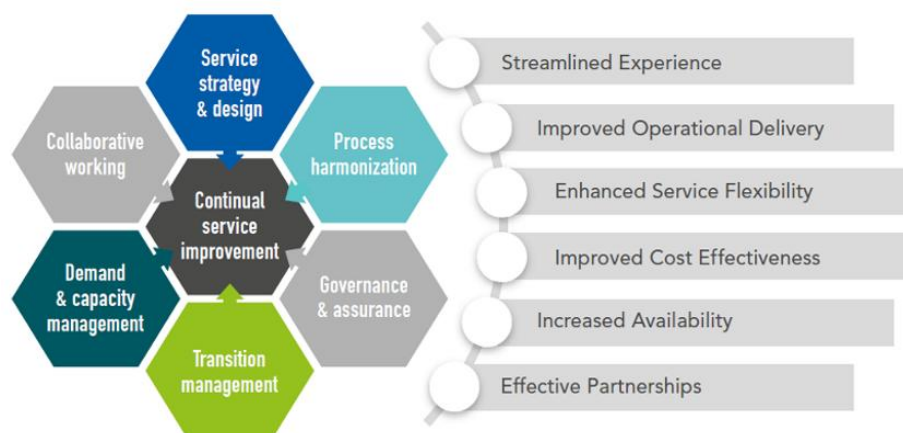
We appreciate the nature of your business demands an exceptional service. We recognise you need to be supported by a team who are not only competent and highly skilled, but also passionate about delivering the right outcome, every time. In our experience, this is achieved by aligning our expertise from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



Your Account Manager will build an understanding of your current and long-term strategy and ensure that the wider Redcentric team understands your needs. They are responsible for the day-to-day commercial relationship between the customer and Redcentric. Our aim is to develop a long-standing partnership with you.

Sharing Technology advancements with you

A key role of your Redcentric account manager is to understand your business and to keep you proactively informed on the technology and industry developments that may be of strategic benefit to you. As part of your monthly service reviews, we will discuss our product and services roadmap and where required involve our technical design resources to better understand your requirement and provide guidance.



Our technology roadmap review forms part of the service delivery programme. Our aim is to ensure you are fully informed of the wider developments that we are planning to introduce and allow us to discuss any requirements you would like us to consider for the future.

Working in partnership to drive continuous improvement.

We fully embrace the continuous service improvement and will work with you to develop a continuous service improvement plan (CSIP). At the simplest level your CSIP will act as a way of prioritising and tracking minor improvement initiatives such as tweaking process to better suit your need but is equally used to drive technology enhancements and innovations to align evolving business requirements, including technology refresh, changes, and upgrades throughout the contract period.

12. Service management

Redcentric will provide a centralised service management model for all services we deliver to you. Our proven model will ensure you receive service management and support services that is easily accessible and effective.

Our mature processes are based on the ITIL framework, fully supported by Gartner-referenced service management tools and process automation which ensures you receive a best-in-class user experience.

The proposed solution is inclusive of our support and account management service, which include:

- Genuine 24/7/365 service desk which is manned, monitored and maintained using as mature ITSM tool
- Best-in-class secure management and monitoring tools, designed to ITIL guidelines.

Our service is underpinned by comprehensive, yet agile, documented processes that include major incident management. We have recently introduced enhanced SLAs within our support services, this means we will respond to you quicker and we are committing to faster fix times.

Service Reviews are an opportunity for us to collaboratively evaluate service performance and ensure it is effective and aligned to your needs. The service reviews seek to understand how we can work in partnership with you and your teams and to identify how we can improve performance. We work proactively to propose solutions to problems and suggest the best way to resolve any issues.



What happens at the monthly service review?

- Review service delivery using performance data and provide this in a graphical format.
- Analyse support tickets to identify patterns that indicate we need to explore further to identify the root cause.
- Review service availability, service exceptions, significant incidents, and related trends.
- Build operational relationships between our customers and the wider Redcentric team.
- Seek to align internal resources within Redcentric to ensure effective service delivery.
- Identify areas for improvement and include them in the service improvement plan.
- Seek your input on how we can evolve our services to suit your future objectives.
- Share our vision to demonstrate how we can support your future strategic aims.
- Create and hold formal records in the Redcentric document management system.

The monthly service pack provides a basis for discussion. It can be tailored to meet specific customer reporting needs as part of the onboarding process or within the lifetime of the contract. As standard, we provide a service pack that includes up to 12 months of data extracted from the support system and service monitoring systems. We analyse current and previous months' performance and identify any trends.

We operate a Service Management System which meets the requirements of ISO/IEC 20000, which means we have a tried and trusted model for service delivery that provides a consistent approach.

13. Support Services

We understand that our customers trust the Redcentric team to ensure that our services meet your needs. Our relationship with our customers goes beyond just complying with contractual SLAs and meeting industry standards.



We seek to understand the importance of service delivery to your organisation and work with you to provide the support that leads to the rapid resolution of any issues.



We take a pro-active approach to supporting you so you can be sure that the services which your business relies on are in safe hands.



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



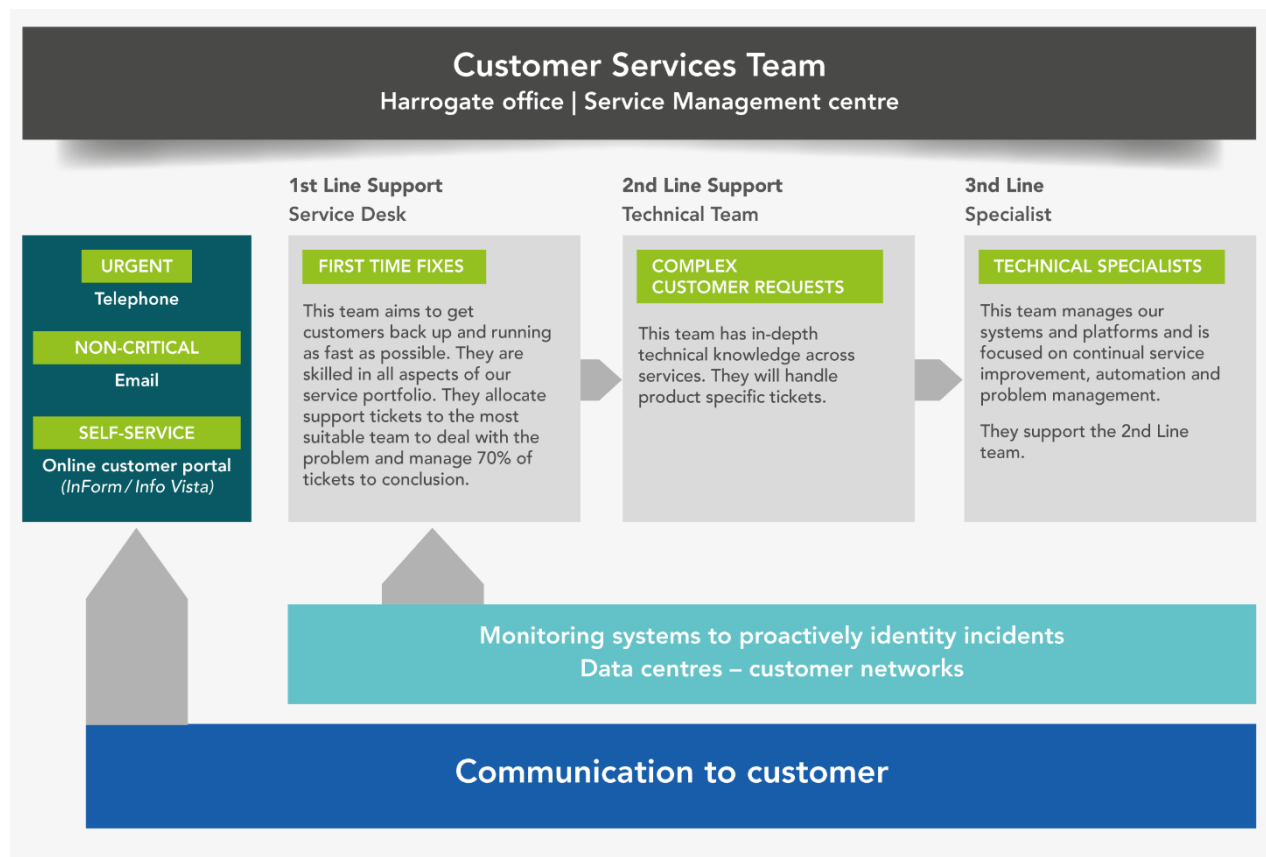
We have thoroughly documented the major incident and customer service plans, which detail how we operate in business-as-usual scenarios and during major incidents.



We use best-in-class secure monitoring tools to manage the services we provide to you actively. We use Gartner-referenced service management tools and process automation, which allow us to work smarter.

Our support function is structured to ensure fast resolution of incidents with timely escalation where appropriate.

The service journey you experience is important to us. Every interaction is monitored by our customer services team, who are highly experienced in handling customer interactions, and understand the importance gathering accurate and timely information to ensure the correct resources are allocated to reach a rapid conclusion.



Our incident management process has been engineered to be customer focused and designed to ITIL guidelines. We follow a proven process for incident management, with clear steps marked out for each team to ensure you are supported in the most effective and organised manner.

14. Information assurance

Certifications

Redcentric are ISO 20000-1 certified, demonstrating that we adhere to ITSM (IT Service Management) best practice, and ITIL (Information Technology Infrastructure Library) provides advice on ITSM best practice.

ITIL v4 is at the heart of Redcentric managed service operation and support. Redcentric believes that to deliver a high quality, professional service it is necessary to invest in training people, empowering them to be strong ambassadors of our service model.

Redcentric has provided managed services to the UK public and private sector for over 30 years. As a highly accredited business, we are proud of the standards and processes for which we are certified.

Our data centres and all supporting operations are fully UK Sovereign and are congruent with;

- The Government's Security Classification Policy ('Official-Sensitive')
- The Government's previous Protected Marking Scheme classification (BIL4 - Confidential)

Note – Redcentric can also support information and assets classified above the GSCP level of 'Official-Sensitive'.

ISO

- ISO 27001:2022 Information Security Certified
- ISO/IEC 27017:2015 Cloud Security Certified
- ISO/IEC 27018:2019 Personally Identifiable Information (PII)
- ISO 9001:2015 Quality Management Certified
- ISO22301:2019 Business Continuity Management
- ISO 14001:2015 Environmental Management System Certified
- ISO 20000-1:2018 IT Service Management System Certified

NHS standards

- Registered HSCN CNSP (Health and Social Care Network, Consumer Network Service Provider)
- DSPT (Data Security and Protection Toolkit) assessed as exceeding standards
- NHS Certified Commercial Aggregator
- NHS Business Partner
- Authorised to transmit, process and store Person Identifiable Data (PID)

- NHS England IGSoC Compliant Commercial Third Party (NACS code: YGMAP)
- NHS England accredited Service Provider (Network Access Agreement number: 0740).

HMG / other standards

- PCI-DSS Compliant for physical hosting and managed firewall services within our data centre locations
- Cyber Essentials Plus Certified
- Data Centres are externally certified to attest they have the necessary physical security measures to process HM Government 'Official-Sensitive' classified data
- Main data centres are certified as Police Assured Secure Facilities
- Full alignment with the Security Policy Framework
- All services are designed, built, implemented, and supported using all relevant and appropriate NCSC GPGs, Cabinet Office and NHS England standards

Networks Connectivity

- The Public Internet via Private or Public IP VPN
- The HSCN Peering Exchange
- PSTN
- PSN (Public Sector Network) certified as one of the few DNSPs (Direct Network Service Provider)
- PSN Gateway Access for both PSN-Assured and PSN-Protected
- JANET (Joint Academic Network)

Further information with regards to the Redcentric assurance and governance framework can be found within the Redcentric customer security pack which consist of the following documents:

- Cloud Security Principles (aligned with the NCSC 14 principles)
- Security Management Plan
- Security Statement
- Accreditations and Mappings (lists all business accreditations and relevant controls and standards utilised for Redcentric G-Cloud services)
- Security Control Framework

Copies are available under NDA upon request.

15. Professional services

The Redcentric Professional Services team is drawn from across the organisation, bringing together a unique mix of experience, know-how and talent to help deliver substantive value to its consulting assignments.

Strategists, designers, developers, technicians, engineers, analysts, security specialists and project managers from the worlds of infrastructure, networks, applications, communications, and mobile can come together to deliver expert, targeted, outcome-driven assistance where it's needed.

The common denominator in every professional services engagement is that we are responding to a specific client need. We provide tailored responses to your requests for assistance, whether that's for help of a strategic or tactical nature, short or long-term, on premises or off, single vendor or multi-vendor environment, in a lead role or in support.

Redcentric provide Professional Services using either our in-house team or approved third parties. Professional Services are not part of the service unless

so specified in the customer's order. Professional Services require a separate order or change control procedure.

Available services

- IT strategy.
- Project management.
- Change management.
- Design integration.
- Staging and installation.
- Integration design.
- Service migration.
- Optimisation and performance tuning.
- Physical lift and shifts.
- Audits and compliance.
- Application development.
- On premise and/or remote access support.

16. Company profile

Redcentric is a managed service provider, delivering highly available network, cloud and collaboration solutions that help public and private sector organisations succeed.

We provide:



Assured availability – Delivering highly available solutions that organisations can rely on to improve productivity and performance



Organisational Agility – Helping organisations to address operational, financial, and regulatory challenges at speed



Smarter Working – Enabling and empowering organisations to connect, communicate and collaborate

Our aim is to work in partnership with you to improve efficiencies, drive transformation and enhance the services you provide to your citizens, patients, students and tenants and our services are provided in line with the most stringent public sector standards.

We are here to support you, whether that be with traditional infrastructure or making the move and taking advantage of what the cloud and hybrid environments have to offer.

Today we can offer a rich end-to-end solution portfolio covering the full spectrum of cloud, network and collaboration designed and delivered by our own highly skilled teams from our privately owned, UK based multi-million pound infrastructure.

Our ethos is one of collaboration; our aim is transformation: helping clients secure desired outcomes, substantive gains, and a measured route forward for the future.

Our assurance comes from a long track record across both the private and public sectors, characterised by deep domain expertise, continuous innovation, proactive management, and an enduring commitment to business improvement through better IT. We'd like to think that there are hundreds of organisations out there where Redcentric has already made a significant and lasting difference.

- Multiple wholly owned UK data centres
- Serving over 800 customers across the UK
- Health and Social Care Network approved CN-SP
- NHS Digital approved N3 Aggregator since 2014
- Accredited to connect and supply over Janet
- Authorised to process HM Government data marked 'Official-Sensitive'
- Accredited to store patient data
- HSCN Peering Exchange Provider
- Accredited to connect and supply over Public Services Network (PSN)
- Accredited and experienced G-Cloud supplier
- 15+ years of N3 experience
- Fully aligned with ITIL Service Management Standards
- ISO 9001, 14001, 27001, 22301 and 20000-1 certified
- Cyber Essentials and Cyber Essentials Plus certified
- PCI Compliant for physical hosting services
- Services designed, built, implemented and supported using appropriate NSCS GPSs, Cabinet Office and NHS Digital standards
- Fully approved HSCN connectivity to Azure and AWS environments.

17. Why choose Redcentric?



Owned infrastructure

We believe that service quality is dependent on end-to-end control and capability, which is why we've spent the past three decades building our own infrastructure and skills base: a UK-wide MPLS network, UK-based data centres, Voice and IaaS platforms, Network and Security Operations Centre, and a large ITIL-based support operation.



Expert guide

We are not about the provision of one-off IT commodities but rather helping clients over the short, medium and long-term through the strategic alignment of our services to organisational requirements. We guide you on your journey at whatever speed and in whatever direction the need dictates.



Customer-centric culture

It is the 'can do' attitude of our teams that we are most proud of and which our customers most value and often comment on. We invest in our staff and work hard to develop and preserve a culture that prioritises staff satisfaction and motivation. We believe that the happier, more engaged, and dynamic we are as a team, the more we can achieve together, ensuring we deliver the best results for our customers.



Open-minded and innovative

We pride ourselves on being an innovative service organisation which means we are always willing to think and do differently and to go beyond norms and conventions. We are always reviewing our proposition, introducing new proven technologies that dovetail with our existing offering; and bringing these opportunities for further gains to our customers. But equally this spirit of innovation may be seen in our flexible approach to project management, and it extends to all aspects of how we work with our customers.



Breadth of services

Our great strength is our ability to be a single unifying partner who can deliver a comprehensive range of IT and Telecoms services across multiple sites with confidence.



Security and integrity

We invest in our systems and processes, that in turn allow us to attain the highest standards of certification and accreditation. These are not badges of honour, but hard-earned evidence of our commitment to quality, security, and integrity, and this supports our aim to be a 'trusted partner'.



Outcomes focused

We believe we have an important role to play in ensuring you have the IT infrastructure and services to help you to achieve your goals. We help you to meet new challenges and to stay agile so that you can respond to change and at the same time keep your data and systems highly secure.



Our teams

We have highly skilled staff, whose average tenure is more than 10 years bringing a huge wealth of experience and a depth of knowledge on which you can rely. We also invest in the development of new team members who bring new or enhanced skills to Redcentric and the training of existing staff to ensure you benefit from a consistent, high-grade delivery of services and support day in, day out.



Continuous Service Improvement

We are committed to investing the most that we can to build a sustainable, successful business that can deliver genuine IT outcomes for our customers. We are continually refreshing our core systems or adding capacity and capability, to the tune of many millions.



Proactive

We think and
act quickly



Inspired

We create
excitement through
innovation

Trusted

We do what
we say we will

Collaborative

We work together
to deliver
a common goal

Transparent

We are open,
honest and fair





Head office

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522

E sayhello@redcentricplc.com

W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED

