Service Definition: Cloud Managed Networking

Crown Commercial Services | G Cloud 15 framework

Contents

Document Information

Client name	G Cloud 15 Service Definition
Project name	Cloud Managed Networking
Document author(s)	David Gearing, Gill Brown

Document Change Record

Issue	Date	Description
V0.1	01/12/25	Draft Template
V0.2	12/12/25	Draft Initial Content added
V0.3	22/01/26	Draft for review and sign off
V1.0	27/01/26	Final for issue

Contact Information

This document has been supplied by Roc Technologies Limited, whose registered office is:	Roc Technologies Limited 1 Lindenmuth Way Greenham Business Park Greenham Thatcham RG19 6AD United Kingdom
Please refer all enquiries to:	**Gill Brown, 0845 647 6000** publicsector@roctechnologies.com.

Confidentiality Agreement
All information contained in this document, including any prices quoted, is to be treated as confidential. It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without the express written permission of Roc Technologies Limited and shall be held in safe custody.
These obligations shall not apply to information that is in the public domain or becomes known legitimately from some source other than Roc Technologies Limited. All intellectual property rights of products or services provided by Roc Technologies Limited shall remain vested in Roc Technologies Limited.

Non-Disclosure
None of the information may be used by the client for any other purpose, nor may it be disclosed by them otherwise than, firstly to members of its staff who will be engaged in the evaluation and, secondly, to representatives of any organisation acting in the capacity of professional adviser to the client. Before making this document available for evaluation, the client must bring this notice to the attention of those concerned.

Proprietary Information
The information in this document has been reviewed and is believed to be accurate. However, neither Roc Technologies Limited. nor its affiliates assume any responsibility for inaccuracies, errors, or omissions that may be contained herein. In no event will Roc Technologies Limited or its affiliates be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect or omission in this document, even if advised of the possibility of such damages.

Roc Technologies Limited reserves the right to make improvements or changes to this document and information contained within, and to the products and services described at any time, without notice or obligation.
Roc Technologies understands that any award to supply the products and/or provide the services that are the subject of this document is subject to the mutual execution of a definitive written agreement.
All information supplied for the purpose of this Roc Technologies document is to be considered confidential.

1. Service Summary

As a solutions aggregator and specialist managed services provider, Roc Technologies (Roc) have been implementing and supporting IT Solutions for over twenty years. We maintain, transform, and manage IT systems that enable organisations to grow and flourish. Whatever the requirement, Roc can manage all your hardware and software needs, from servers and desktops to applications, data, and networks. We support our customers throughout the IT lifecycle, from initial strategy development and technology assessment - through to innovative design and procurement processes, implementation, and management.

Networking and Connectivity is a core part of Roc's Platform business unit. We are responsible for managing service for some of the UK's largest networks and most secure modern networks.

Roc offers a wide range of network services including full transformation of wired, wireless, remote access, network access control, and security implementations for campus and data centre and migration to cloud management. We meet all scales of network requirements from ad-hoc consultancy to full infrastructure transformation programmes. We have a skilled Project and Engineering base who provide full end-to-end project delivery for network implementations. We can provide RF surveys, cabling, design, implementation, consultancy, support and manged service.

Roc's Cloud-Managed Networking offers deployment and cloud-scale orchestration of customers infrastructure. Infrastructure includes industry-leading vendors of LAN, Wi-Fi, Security, Remote Access and SD-WAN solutions which may be an existing deployment or a network refresh supplied and provisioned by Roc.

Features and benefits of a Roc's cloud-managed network offering are described below.

- Design, supply and provision of network and security solutions.
- Unified management of wireless, wired, VPN, and SD-WAN.
- Centralised control functions orchestrating configurations and software.
- AI-based operations for faster root-cause analysis and continuous network optimisation.
- Network reporting, analytics and insights.
- Integration with User Experience Insight to proactively monitor and improve the end-user experience.
- Intent-based policy engine and access controls to strengthen and simplify security at scale.
- Inline client profiling and telemetry to close visibility gaps associated with IoT.
- Powerful monitoring and troubleshooting for remote or home office networks.
- APIs and webhooks to augment the value of other leading IT platforms in your environment.
- Live Chat and an AI-based search engine for an enhanced support experience.
- Accredited engineers for best practice, vendor validated design and installation.

2. Service Description

Roc works with leading network vendor technologies to design, deploy, manage and support customer infrastructure. Roc's Cloud-Managed Network offering includes the following service capabilities:

Network hardware scoping, design and delivery:

- Requirements scoping and solution design for modern network connectivity.
- Hardware/software/VM supply and provision including LAN switches, Wireless Access Points, Controllers/Gateways, NAC, Security, SD-WAN.
- Cloud-management with on-premises options available.
- Roc work with leading vendors to best recommend the technology most appropriate to the technical requirements and to meet customer choice.
- Vendor accredited engineers for best practice and supportable designs.
- Deployment of campus fabric such as EVPN-VXLAN for scalability, flexibility and security.
- Secure network separation of Corporate, Guest, 3rd-party and IOT devices.
- Zero-Trust and Network Segmentation architecture.
- Location Services and User-Engagement capabilities.
- Professional Services to undertake installation and configuration.
- Cabling and RF Survey services.
- Monitoring and Managed Services.

Management and Orchestration:

- Scalable, cloud-hosted management of network infrastructure
- Zero-touch provisioning
- Templated configurations for design consistency
- Software-driven security and access orchestration
- Cloud authentication options

Analytics:

- Robust dashboards, reports, and audit trails to maintain quality of service and compliance with IT policy
- Visibility and control over all your locations
- Improve network performance based on user, application, and device experience
- Gain organisation insights and intelligence through network data analysis

Automation and Programmability:

- Programmable services architecture
- Simplify network configuration through programmable tasks using Ansible and Python scripts
- APIs and Webhooks support 3rd party integrations to enhance operations and security
- Auto-remediation capabilities and recommended actions through AI insights

AI Operations:

- Advanced AI/ML techniques provide enhanced detection and visibility of network-connected client devices
- Enhanced client identification using machine learning-based classification and behavioural analytics
- AI Insights to pre-empt network issues, provide remediation steps or take automated actions
- Natural Language Processing (NLP) help and search functions
- Automated packet captures and ticketing for troubleshooting and Support desk integration

User and Device Experience Insights:

- Sensor-based network performance tests provide continual experience monitoring
- Simulate actual user experience by seeing what users see when using different apps
- Test and validate all aspects of connectivity including LAN, Wi-Fi and WAN
- Root cause identification and analysis

Network Access Control:

- Comprehensive NAC and AAA capabilities (Authentication, Authorisation and Accounting)
- Granular policy enforcement and role-based access
- Workflow Guest captive portals
- Full branding and customisation
- Integration with 3rd party integration solutions (e.g. firewalls, MDM, SIEM) to expand control
- Support for multi pre-shared key (MPSK) for simple multiple device onboarding

Performance:

- Wide range of network hardware to meet all scales of customer network requirements
- Switch virtualisation technologies and stacking for scalability, redundancy, and high availability
- High-performance and capacity Wi-Fi based on Wi-Fi 6, 6E and 7 standards
- High-speed backbone connectivity including Multigigabit copper ports and modular 10/25/40/100GbE uplinks
- Cloud-controlled and Gateway-controlled wireless options

Monitoring and Reporting:

- Comprehensive device monitoring through dashboards
- Network health status including device status, memory, CPU, channel utilisation, channel noise
- Network topology and heatmap views
- Configurable parameter thresholds and alert triggers
- Standard and customised reports
- Various export formats - PDF, CSV, Email

2.1 Product Portfolio

2.1.1 HPE Juniper Wired and Wireless Networking

In today's hyper-connected world, businesses demand more than just a network—they require a digital backbone that is robust, agile, and secure. HPE Juniper Wired and Wireless Networks, the industry leader in delivering cutting-edge solutions, is revolutionising the way businesses connect, collaborate, and compete.

With Juniper Mist micro-segmented cloud-based management, businesses gain access to a groundbreaking AI-driven platform that delivers unparalleled insights, automation, and user experiences. By harnessing the power of AI and machine learning, Juniper Mist simplifies network configuration and management, predicts and resolves issues before they arise, and optimises performance across the entire network stack.

With HPE Juniper Networking, Roc can deliver a seamless, reliable connectivity experience to your employees, customers, and partners alike.

2.1.2 HPE Aruba Wired and Wireless Networking

Introducing HPE Aruba Networking Products: Elevate Your Connectivity Experience to New Heights.

With a focus on innovation, reliability, and simplicity, HPE Aruba offers a comprehensive portfolio of networking solutions designed to meet the diverse needs of modern enterprises. From access points to switches to controllers, every HPE Aruba product is engineered with the end-user in mind, delivering an unparalleled connectivity experience that is fast, reliable, and seamless. With advanced features such as intelligent traffic management, self-optimising Wi-Fi, and AI-driven analytics, HPE Aruba products empower businesses to deliver a superior user experience that drives productivity and satisfaction.

HPE Aruba products are built for scalability and flexibility, allowing businesses to easily adapt to changing needs and requirements. Whether you're a small business looking to expand your network or a large enterprise with complex infrastructure demands, HPE Aruba offers solutions that can grow and evolve with you, without compromising on performance or reliability.

2.1.3 HPE Aruba ClearPass Network Access Control

ClearPass specialises in dynamic Network Access Control (NAC), enabling granular policy enforcement based on users, devices, and applications, ensuring a secure network environment that aligns with Zero Trust architecture principles. ClearPass provides a dynamic and automated approach to access control, serving as the central point of authority enhancing security.

2.1.4 Palo Alto Firewalls

Palo Alto firewalls are designed to deliver optimal security and granular policy enforcement. By integrating Palo Alto firewalls into our solution, we can ensure a secure, reliable, and resilient network that is built on the foundation of Zero Trust principles. Palo Alto provides advanced cybersecurity solutions, with session identification and policy management capabilities. Devices can be orchestrated and managed from the cloud.

2.1.5 Fortinet FortiGate Firewalls

With a comprehensive suite of advanced security features and unmatched performance, FortiGate Firewalls offer a holistic approach to network security that goes beyond traditional firewalls. FortiGate Firewalls offer an integrated security fabric, that provides seamless protection across the entire network infrastructure. From the edge to the cloud, FortiGate Firewalls offer consistent, real-time threat intelligence and enforcement, ensuring that every corner of your network is safeguarded against cyber threats. FortiGate Firewalls also offer unparalleled ease of management with both cloud and on-premises management options streamline security operations, saving you time and resources.

2.2 Service Delivery

Roc offers packaged services for moving customers to a Cloud-managed network, using the approach below:

2.2.1 Support Model

The services within this document are designed to operate as a 2nd or 3rd line resolver group behind the client's principal end-user service desk. Where the client uses a separate desk, Roc expects that the clients service desk will employ reasonable efforts to 1) eliminate end-user error and 2) identify the most appropriate resolver group.

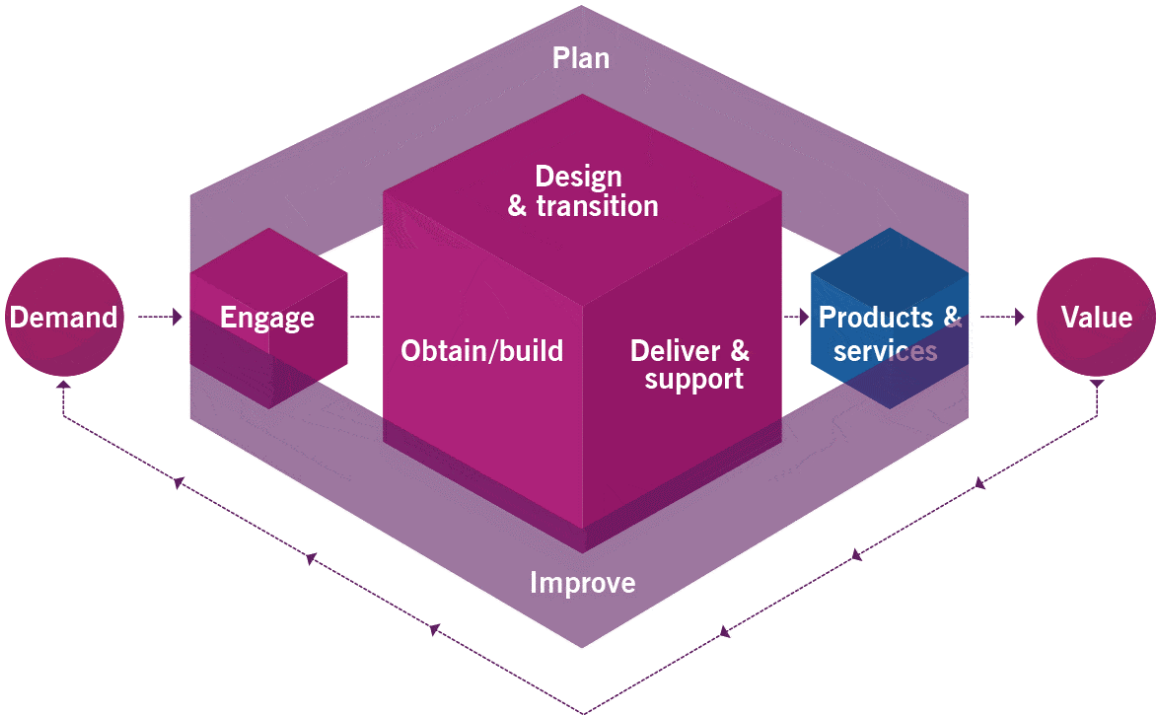
Additionally, where a separate 1st line desk is in use, Roc request that the clients service desk will operate during the same hours as the selected Roc service and manage communications amongst client stakeholders.

2.2.2 Accreditations & Vetting

Roc's services are delivered from Roc's UK based Technical Operation Centre (TOC) and a dedicated Security Operation Centre (SOC). All team members are DBS and BPSS checked and where required, Roc are also able to provide SC and DV cleared resources.

Services are delivered in alignment with ITIL and Cyber Essentials standards, as well as ISO 20000, ISO 27001, ISO 9001 and ISO 14001.

Roc's commitment to aligning with industry best practices and ensuring the highest standards of service management, information security, and cybersecurity are paramount in our approach to delivering services. We confirm our alignment with ITIL V4 principles, our ISO27001 accreditation, and our Cyber Essentials Plus certification, underscoring our provision of a secure, efficient, and customer-centric service delivery model.



2.2.3 Support Mechanism

As a matter of routine, all services are delivered remotely. Roc assumes that an existing, industry standard remote access mechanisms will be available, via the internet, SD-WAN, PSN, N3, RLI or dedicated client WAN. Roc also offers a range of optional field engineering services where required to support hybrid cloud components such as network infrastructure or private cloud platforms.

2.2.4 Support Agreements

To provide best value and consistent pricing, the services described within this document assume that existing customer software/provider/manufacturer support or warranty agreements will remain in-place and be accessible by Roc to facilitate a swift response to any security issues raised around third-party offerings.

2.2.5 Service & Operational Tooling

Roc can provide access to our own service and operational management tools or leverage clients existing tool sets. Roc will require appropriate remote access and licences where client tools are leveraged.

2.2.6 Change Management

It is assumed that each in-scope supported item will be fully managed by Roc, in line with the agreed change management process. Whilst the client and other 3rd parties chosen by them can retain administrative access (e.g. for emergency/auditing purposes), it is assumed that all changes to an in-scope supported item will be performed by Roc.

One hour of change management time per month is included for each in-scope supported item. This will be fulfilled during normal business hours. Additional service points can be purchased as required for the fulfilment of additional services.

2.3 Service Level Agreements

The below table summarises the SLAs offered as part of Roc Managed Cloud Services.

2.3.1 Hours of cover

Roc's Managed Services are offered based upon two standard hours of cover-

- Normal Business Hours: Monday to Friday, 08:00-18:00, excluding public holidays
- 24x7: 24 hours per day, 7 days per week, 365 days per year

2.3.2 Incident Management

Priority	Definition	Target Response	Target Update	Target Resolution
P1 (Critical)	Critical Business Impact. A complete service failure or severe degradation of service. Typically impacting >50% of users at a supported site, or >50% users of a supported system. No acceptable workaround available. Examples include: - • Complete network failure • Simultaneous failure of resilient WAN links • Core application/service down	15m	30m	4h
P2 (Serious)	Serious business impact. A widespread degradation of service, typically impacting all or a significant number (>25%) of users at a supported site, or of a supported system. Examples include: • Severe network performance degradation • Severe application performance degradation • Failure of non-resilient WAN links • Extended application functionality failure for all users • A loss of system resiliency	30m	1h	6h

P3 (Medium)	Medium business impact, A partial or intermittent degradation of service. Typically impacting a subset, group, or individual system users. Examples include: • Partial/intermittent network degradation • Partial/intermittent application degradation • System failure impacting individuals • Extended application functionality failure	2h	10h	16h
P4 (Low)	Low/minimal business impact. Typically, non-critical loss of service/functionality, or minor degradation of service for individual users. Examples include: • Network issues affecting lab/test Equipment • Applications issues when testing changes • Partial application degradation for individuals • Threshold breeches with no impact on service.	10h	20h	40h

2.3.3 Change Management

Definition	Target SLA
'Standard' Change Request List to be agreed during service initiation and regularly reviewed/updated during service operation	**5 Days** - to complete
'Non-Standard' Change Request*	**10 Days** - to complete

2.3.4 SLA Terms

1. The SLA times within the above tables are offered as a target time against which Roc's performance will be assessed.
2. The SLA clocks will run during the agreed hours of cover. Where 24x7 cover has been purchased the SLA clock will run outside of normal hours for P1 & P2 incidents only
3. Where the priority of an incident cannot be agreed, the client's decision will apply. Should this occur frequently, it will be addressed during the service review meetings.
4. All incident requests will be logged within the agreed service management toolset. A minimum data set will be mutually agreed for a request to be logged. An incident request will be considered as 'logged' once the clients service desk has documented the minimum dataset and assigned the request to Roc's resolver group.

5. The 'Response' SLA is measured from the time at which an incident is 'logged' to the time at which its status changes to 'Work in Progress', typically because: Remote investigation has commenced.
6. The 'Resolution' SLA is measured from the time at which an incident is 'logged' to the time at which its status changes to 'resolved'.
7. Incident 'Updates' will be provided via ticket updates, phone, voicemail, email or in-person dialogue with customer contacts.
    - SLA clocks will be paused if a request cannot reasonably be progressed for reasons outside of Roc's control.
    - Awaiting further information from the client and thus no progression is possible.
    - Awaiting onsite engineering support.
    - Awaiting testing confirmation from the user/requestor.
    - Awaiting client approval for additional costs.
    - Awaiting a third party or manufacturer action which is outside of Roc's direct control.
    - Awaiting the completion/approval of a relevant change request.
8. The incident SLA clocks will also be paused if an acceptable work around is implemented, and the priority level reduced.
9. Roc will require the ability/authority to liaise directly with any in-scope software vendors, manufactures of service providers, to obtain software updates or TAC support.
10. A Major Incident Report (MIR) will be provided within 5 working days for any P1 or P2 incident which exceeds the committed SLA's, exhibits a process failure or where there is a clear opportunity for service improvement.
11. During the service provision, systems will be maintained at supported software versions and in line with manufacturer best practice. From time-to-time Roc may also make recommendations to improve the security, performance, or availability of an in-scope item.

2.4 Service Delivery Management

Roc provides two standard packages of service delivery management 'Standard' and 'Enhanced'.

Package	Description
Standard	• Standard Roc Service Report Template. • Quarterly service review performed remotely.
Enhanced	• Customised/Bespoke service report template • Monthly or quarterly service reviews performed remotely. • Quarterly onsite service reviews with aligned SDM.

	• Tailored observations & recommendations. • Continual Service Improvement Plan (CSIP).

Roc will incorporate standard service reporting within the scope of a Managed Service. The service reports will cover the following:

- A summary of all incidents and service requests logged with the Service Desk.
- A list of outstanding incidents and service requests and their status.
- Roc's performance against the service levels in the relevant month.
- Updates to agreed MIR remedial actions.
- 3rd party performance against their committed service levels.
- Quantitative and qualitative service reports/graphs.
- Infrastructure reports with relevant information on capacity, performance, and availability.
- Support advisories (for example end-of-life statement and upgrade recommendations).
- Software advisories (for example recommended updates).
- General observations and recommendations.

2.5 Continuous Improvement

Roc places high value on the delivery of Continuous Service Improvement (CSI) and Customer Experience to drive business value and efficiency. CSI will be driven by Service Delivery Manager and Account Manager. Each service improvement item will define the business outcomes and be driven by key metrics around customer value and experience.

We would continually monitor SLA and KPI performance throughout the contract term and provide reporting through Service Reviews. In terms of contractual remedies, the key premise is this should be measured against SLA and KPI performance.

3. Service Pricing

Refer to Roc's pricing document representing service costs.

3.1 Onboarding Fees

For each new service provision, a one-time on-boarding charge will apply. This fee is charged to cover transition activity such as process definition, toolset configuration, system discovery, remote access configuration and knowledge management tasks. This charged will be in line with Roc's published SFIA Rate card and will vary based upon the nature and complexity of the environment to be on-boarded.

During the on-boarding process, Roc will review the configuration of each in-scope item. Where in-scope items have not been configured in-line with best practice, remedial actions may be required before the item can be on-boarded or covered by Roc's SLA's. Such remedial activity can be performed by the client or Roc. Where performed by Roc it can be funded via Roc's published SFIA Rate card or the Additional Service Points purchased as part of the service.

Roc follow a mature service transition process for on-boarding new Managed Services:

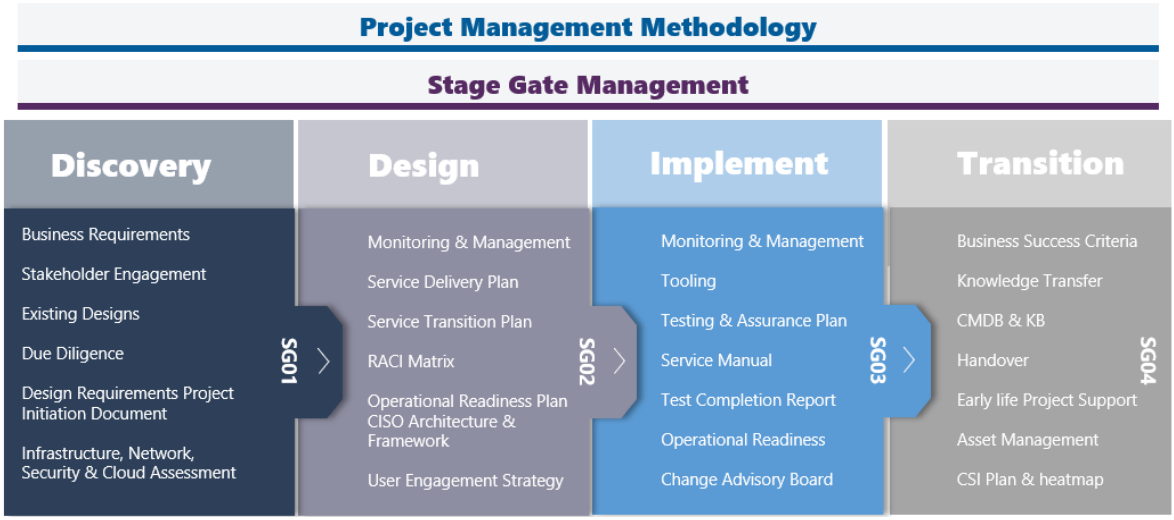


Figure 1 – Roc Service Transition Process

4. Terms and Conditions

Refer to Roc's Terms and conditions documents included with the submission. Standard terms are relevant to smaller one-off purchases, and the Master Service Agreement (MSA) is applicable for longer term contracts.