Service Definition: Cloud Management

Crown Commercial Services | G Cloud 15 framework

Contents

1. Service Summary 5
2. Service Description 7
2.1 Cloud Network Infrastructure Management 7
2.2 Cloud Server OS Management 8
2.3 Cloud Application Management 8
2.4 Availability & Capacity Monitoring and Reporting 9
2.5 Cloud Protective Monitoring 10
2.6 Service Delivery 10
2.6.1 Support Model 10
2.6.2 Accreditations & Vetting 11
2.6.3 Support Mechanism 11
2.6.4 Support Agreements 11
2.6.5 Service & Operational Tooling 11
2.6.6 Change Management 11
2.6.7 Hours of cover 11
2.7 Service Level Agreements 12
2.7.1 Incident Management 12
2.7.2 Change Management 13
2.7.3 SLA Terms 13
2.8 Service Delivery Management 15
3. Service Pricing 16
3.1 Onboarding Fees 16
4. Terms and Conditions 17

Document Information

Client name	G Cloud 15 Service Definition
Project name	Cloud Management
Document author(s)	Lee Gothard, 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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without the express written permission of Roc Technologies Limited and shall be held in safe custody.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

Cloud Management from Roc is engineered specifically for organisations embracing digital transformation and delivering true cloud-native applications. Within its role as a Managed Service Provider, Roc has extensive experience in the design, implementation and management of Cloud systems and services including Infrastructure as a service (IaaS) and Platform as a service (PaaS) delivered under Microsoft Azure.

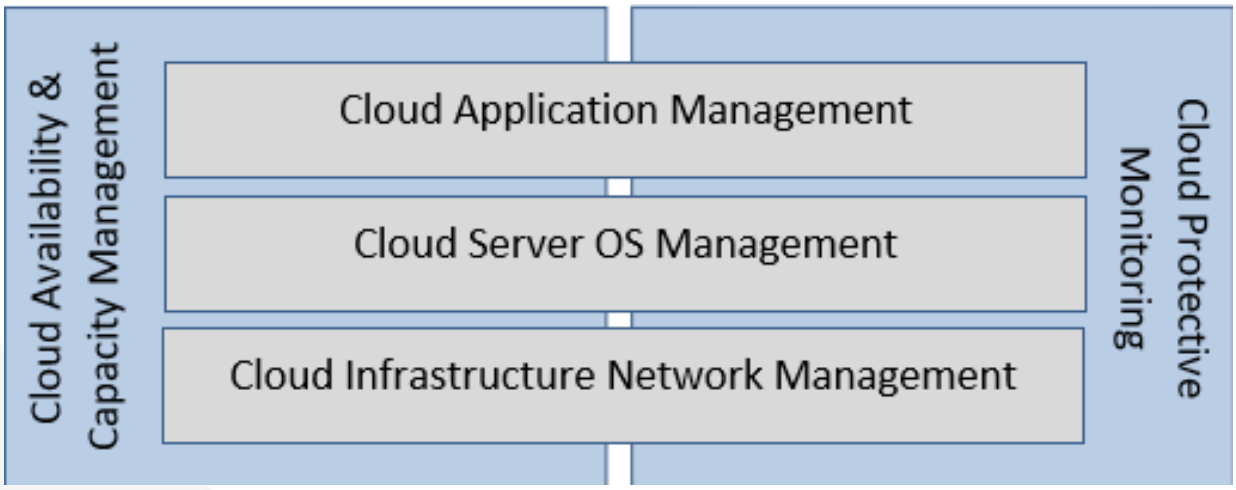
Many organisations prefer not to move their entire IT infrastructure to the public cloud, opting instead to retain some on-premises systems or adopt a private cloud approach. Therefore, we can tailor our service management offering to suit most environments, offering a cloud only or hybrid management service as required.

Roc provides flexible cloud transition services, ranging from partial to full migration focused on optimising cost and performance. A like-for-like migration rarely delivers savings and can often increase costs; therefore, we work closely with clients to identify workloads and services best suited for the cloud, ensuring a cost-effective migration strategy and ongoing cost management. Roc can also provide an AI-powered SaaS platform designed to help organisations optimise cost, security, usage, and compliance across their Azure and Microsoft 365 environments. It goes well beyond native tools like Microsoft Cost Management by offering deeper analytics, proactive recommendations, and governance insights.

Roc's Managed Cloud services provide G-Cloud customers with a range of modular support packages for public, hybrid and private cloud infrastructure, operating systems and applications.

These services are underpinned by Roc's UK based managed services team and delivered in line with ITIL and Cyber Essentials best practice.

The service modules available can be summarised as:



The above standard service modules are offered based upon a fixed number of points, per supported item, per month. Each point costs £1. Additional service points can then be purchased for the completion of planned changes, out-of-scope activity and additional proactive services / scheduled tasks.

Roc's Managed Cloud Services are offered with a choice of SLA and Service Delivery options. They can also be configured to consider:

- Client specific operational processes.
- Complex or custom applications.
- The use of client owned service management and operational tooling.
- Enhance information assurance requirements – such as SC or DV clearance.
- Enhanced service delivery reporting.
- Cloud compliance information and reporting.
- Continual service improvement for your Cloud environment.
- Improved visibility for your Cloud environment.
- Adaptive transformation to your Cloud environment.
- Service governance for your Cloud environment
- Business value and outcomes based delivering Cloud success.

Client specific processes are underpinned by Roc's Process Management platform, providing Agile support and projects for your Cloud environment. During the service initiation and transition, Roc will map all applicable processes, capturing all inputs, outputs, and work instructions for each task within a process. Working together to provide an effortless experience for users and customers for your Cloud and hybrid estate.

2. Service Description

Roc's Managed Cloud Services are based upon a range of modular support packages which have been designed for public, hybrid and private cloud infrastructure, operating systems and applications.

2.1 Cloud Network Infrastructure Management

Roc's Cloud Network Infrastructure Management is intended to provide operational management for network infrastructure components running on or underpinning cloud solutions. This includes physical and virtual routers, switches, firewalls, load balancers and security appliances. The service includes the following features:

- OS an application Incident and Problem resolution (including escalation management)
- OS and application patch management
- Daily operational checks
- Change Management (up to 1 hour per month, during normal business hours)

The service assumes that in-scope device is integrated into existing operational management tools. The service also assumes that the devices are configured in line with security best practice.

Patching will be performed during agreed maintenance windows, in line with the agreed change control process. Where applicable it will be implemented using client owned operational tools installed within the client's cloud environment. Where possible, patches will be scheduled for automatic installation; however, where supporting manual activity is required this will be deducted from the change management time allocation or additional service points.

Roc's Cloud Network Infrastructure Management is charged per network device/instance and is offered for 'standard', 'Medium complexity' and 'high complexity' devices:

Server type	Description
Standard	Edge/access layer switches, standard WAN routers etc.
Medium Complexity	Edge/access layer aggregation switches, DC/server switches, standard/branch firewalls, HA appliances etc.
High Complexity	Core/complex switches & routers, centralised/complex firewalls, security appliances, load-balancers, Proxy appliances etc.

2.2 Cloud Server OS Management

Roc's Cloud Server Operating Systems Management is intended to provide operational management support for Microsoft and Linux operating systems running on cloud-based server platforms. The service includes the following features:

- OS Incident and Problem resolution (including escalation management).
- OS Patch Management.
- Daily operational checks.
- Change Management (up to 1 hour per month, during normal business hours).

The service assumes that in-scope server Operating Systems will, where possible, be AD Domain joined and integrated into existing operational management tools (e.g. Intune/SCCM/WSUS). The service also assumes that the server is secured in-line with best practice and protected by a reputable industry standard antivirus solution.

OS patching will be performed during agreed maintenance windows, in line with the agreed change control process. Patches will be implemented using client owned operational tools installed within the cloud environment. Where possible, patches will be scheduled for automatic installation; however, where supporting manual activity is required this will be deducted from the change management time allocation or additional service points.

Server OS Management is charged per operating system instance and is offered for 'standard' and 'Complex' server roles:

Server type	Description
Standard	Single domain joined server, confirming to a standard build and built in line with manufacturer best practice.
Complex	HA/clustered servers, mission critical servers, isolated servers with specific security roles, non-standard build or legacy operating systems

2.3 Cloud Application Management

Roc's Cloud Application Management is intended to provide operational management support for hosted application operating systems running on cloud-based server platforms. The service includes the following features:

- Application Incident and Problem resolution (including escalation management)
- Application Patch Management
- Daily operational checks
- Change Management (up to 1 hour per month, during normal business hours)

The service assumes that in-scope server applications will be AD joined and integrated into existing operational management tools where applicable. The service also assumes that the application server is secured in line with best practice and protected by a reputable industry standard antivirus solution.

Application patching will be performed during agreed maintenance windows, in line with the agreed change control process. Patches will be implemented using client owned operational tools installed within the cloud environment. Where possible, patches will be scheduled for automatic installation; however, where supporting manual activity is required this will be deducted from the change management time allocation or additional service points.

Server application management is charged per application server and offered for 'standard', 'Medium complexity' and 'high complexity' applications:

Application type	Description
Standard	AD, File, Print, Exchange, Skype (IM & Presence only), SCCM[2], AV Management etc.
Medium Complexity	Citrix[3], Database[4], Load Balancing/Proxy apps, Backup applications, Skype (with Enterprise Voice), Security appliances.
High Complexity	BPM, Automation, Custom applications etc..

[1]A Discount of 25% applies to all identically duplicated application servers. E.g. Citrix presentation servers.
[2]An additional 'standard app' charge will apply for each managed SCCM Desktop build image and each packaged application
[3]An additional 'standard app' charge will apply for each Citrix desktop build
[4] Databased app management only – excludes DBA services.

2.4 Availability & Capacity Monitoring and Reporting

Roc's Cloud Availability & Capacity Management service provides detection of potential or current service impacting incidents. Upon detection of an issue, Roc will escalate to nominated client contacts and/or commence immediate incident resolution for in-scope supported items.

Capacity data will typically include CPU, Memory, HDD and bandwidth consumption and will be used to underpin Roc's service delivery reports. It will help identify possible cost savings due to over provision or to identify areas where additional capacity may be required.

Roc's Cloud Availability & Capacity Management service can be fulfilled using client or Roc owned tools. The service does not include any additional virtual server hosting or operating system licences which may be required to host the monitoring tools. Where applicable, this can be purchased as part of the service provision.

During the service initiation, Roc will work with clients to determine the key monitoring elements that need to be configured to derive the maximum value from the service.

2.5 Cloud Protective Monitoring

Roc can provide Protective Monitoring in line with GPG13. These services are delivered from a dedicated UK based SOC which operates independently from Roc's Technical Operation Centre.

The service can support infrastructure, operating system, application and custom log sources, and features:

- GPG13 Protective Monitoring
- Forensic log collection, storage, and management.
- Security event monitoring, analysis, reporting and alerting.
- Configuration audit.
- File integrity monitoring and system baseline change monitoring.
- Compliance monitoring.
- File based targeted threat assessment.

One or more log collectors will be required within the client environment and where applicable, this can be provisioned as service.

2.6 Service Delivery

Roc Cloud management services are delivered using the approach below:

2.6.1 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. Roc expects that the client's service desk will employ reasonable efforts to 1) eliminate end-user error and 2) identify the most appropriate resolver group.

Additionally, Roc request that the client's service desk will operate during the same hours as the selected Roc service and manage communications amongst client stakeholders.

2.6.2 Accreditations & Vetting

Roc's Managed Cloud services are delivered from Roc's UK based Technical Operation Centre (TOC) and a dedicated Security Operation Centre (SOC). All team members are 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.

2.6.3 Support Mechanism

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

2.6.4 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. For example, should Roc provide support for a client's Citrix XenApp environment, Roc would expect to leverage the client's existing software subscription agreements to access software updates or Citrix TAC. Should these not be in place, Roc can provide support agreements for most major vendors.

2.6.5 Service & Operational Tooling

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

2.6.6 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.

2.6.7 Hours of cover

Roc's Managed Cloud 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

2.7 Service Level Agreements

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

2.7.1 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	2h	10h	16h

	• Extended application functionality failure			
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

2.7.2 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

2.7.3 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 tool. A minimum data set will be mutually agreed for a request to be logged. An incident request will be considered as 'logged' once the client's service desk has documented the minimum dataset and assigned the request to Roc's resolver group. It should be noted that P1 & P2 incident should also be followed up with a phone call to Roc's Service Desk.

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 in the event that 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 in the event that an acceptable work around is implemented.
9. The scope of the proposed service excludes the support of individual end users and end user devices. The client's service desk will be required to log end-user incidents and perform initial diagnostics to check there is no fault with any element not managed by Roc, e.g. user error, faulty end user device, local power, application functionality. Whilst Roc will liaise with individual end users to resolve infrastructure related issues, this will be on an exception basis, as the primary interface for end users is expected to be the client's service desk
10. The client's staff are required to provide reasonable (just, rational, appropriate, ordinary or usual in the circumstances) local assistance to aid Roc's remote diagnosis. In particular, by checking devices/infrastructure not managed by Roc, performing basic tests and sharing test results.
11. 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.

12. Any failure by the client or Roc to adhere to the obligations set out in these terms will be reviewed and discussed during the monthly service review meetings. Repeated failure may result in applicable SLA's being suspended until a corrective action plan is mutually agreed and implemented.

13. 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.

14. 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 performance or availability of an in-scope item. Clients are required to ensure they have purchased sufficient 'Additional Service Points' to implement changes and recommendations. Roc reserves the right to suspend SLA's if best practice recommendations are not implemented.

2.8 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 via WebEx
Enhanced	• Customised/Bespoke service report template • Monthly service reviews performed remotely via WebEx • Quarterly onsite service reviews with aligned SDM • Tailored observations & recommendations • CSIP content

3. Service Pricing

Refer to Roc's pricing document.

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, systems configuration, system auditing, remote access configuration etc. 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.

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.