Service Definition: Azure Services

Crown Commercial Services | G Cloud 15 framework

Contents

Document Information

Client name	G Cloud 15 Service Definition
Project name	Azure Services
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 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.

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

Roc has extensive experience in the design, implementation and managing of Cloud systems and services. Roc has been a Microsoft Partner for Cloud, Data Centres, Communications and Security for a number of years. We can assist clients at all points of the process of moving to the Cloud, from high level design through to low level design, implementation, migration, and day to day running of Microsoft Azure Cloud services, offering proactive cloud advice to clients.

Roc offers the following core capabilities and services around Cloud services:

- Public Cloud.
- Hybrid & Private Cloud (Hyper-Converged Infrastructure (Azure Local), Servers, Storage, Data Centre Networking etc).
- Cloud connectivity (cloud managed Wired, Wireless, LAN & WAN).

Roc's core Public Cloud offerings focus on Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). In addition, Roc helps organisations modernise traditional client-server applications by transitioning them to the cloud, leveraging SaaS alternatives where available.

IaaS is principally provided through Microsoft Azure, in addition PaaS services are offered for solutions such as Low-code, firewalls and SQL Server, whilst several SaaS solutions are commonplace such as O365, Sophos, Commvault and zScaler.

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. 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.

2. Service Description

A successful move to public cloud platforms such as Azure begins with a clear understanding of the application estate. It is best practice for any organisation migrating its IT infrastructure, or even a single application, to conduct a cloud readiness assessment. This ensures a smooth transition and establishes a cloud environment aligned with business requirements. Roc brings extensive experience in both process and technology to support this critical step. Cloud migration represents a significant investment and demands considerable time and effort from IT teams, making thorough planning essential."

Organisations that prepare thoroughly for cloud migration and develop a clear, structured plan can significantly reduce both time and cost. Roc partners with clients to create these plans, ensuring a strategic approach. Importantly, cloud migration should not be treated as a simple 'lift-and-shift' exercise that replicates existing server-based workloads in the cloud. Instead, workloads should be optimised to leverage Azure capabilities such as Software-as-a-Service (SaaS), where billing is based on software usage rather than underlying virtual machines, and reserved instances, which offer cost savings in exchange for reduced flexibility. Roc provides expert guidance throughout this process to maximise efficiency and value."

A critical aspect of Azure optimisation is evaluating the current application portfolio and determining the most effective approach for cloud migration. In some cases, application vendors may already offer cloud-based versions that provide a cost advantage by leveraging the economies of scale inherent in shared platforms. Alternatively, Azure's expanding Software-as-a-Service ecosystem may present native options. However, it is essential to assess migration implications thoroughly, as certain limitations or incompatibilities may make a server-based solution within Azure the preferred choice. Roc works closely with clients to review workloads and identify the most suitable and cost-effective strategy.

Migrating workloads to the public cloud introduces specific challenges that must be identified and addressed during the assessment phase. Key considerations include security and governance of cloud environments, management policies, and long-term maintainability.

2.1 Azure Cloud Adoption Planning

The Cloud Adoption Framework for Azure provides comprehensive documentation, technical guidance, best practices, and tools to align business objectives, organisational readiness, and technology strategies. This alignment enables a structured, actionable journey to the cloud that delivers on desired business outcomes.

Roc's Cloud Adoption Planning and Assessment follows the principles of Microsoft's Cloud Adoption Framework (CAF), offering a holistic approach to cloud adoption that encompasses planning, readiness, migration, and ongoing governance and management.

Cloud adoption fundamentally changes how organisations procure and consume technology resources, enabling them to provision services on demand. While the cloud offers significant

flexibility in design and deployment, successful adoption requires a proven, consistent methodology.

The Microsoft Cloud Adoption Framework (CAF) provides that structure, helping Roc guide clients through each stage of the journey to accelerate business outcomes. The framework defines key areas that Roc and the client must address to deliver a successful migration, covering the full lifecycle, from planning and readiness to transition, governance, and ongoing management, aligned with Roc's Cloud Adoption Planning and Assessment process.

- Document the Client business strategy.
- Align required partner support.
- Gather client data and analyse assets and workloads.
- Work with client to deliver a business case if required.
- Work with client to create a migration plan.
- Work with client to build a skills readiness plan.
- Roc to deploy and align the landing zone.
- Cloud migration.
- Hand off production workloads to cloud Management.

2.2 Azure Cloud Migration

For a successful Azure Cloud migration, the output of the cloud adoption planning discovery phase would be used to assess the readiness/suitability of services for migration to the Microsoft Azure cloud.

IaaS would be considered for services where no SaaS or PaaS option is available or available options are unsuitable.

Roc would then work with the client to identify the most efficient tooling to conduct migrations, however Azure Migrate is likely to be favoured for most cloud migrations.

Servers /services would then be migrated to the cloud in a phased manner. To achieve the results and the return on investment, the migration needs to be successfully delivered on time and within budget. Roc places an emphasis on delivering effective Project Management for the migration process.

Roc's Project Management approach is designed to make a real difference, and deliver real benefits:

- Better results: The transition delivered successfully on time, within budget and to agreed objectives.
- Reduce risks: Potential risks are pro-actively identified and managed throughout the migration to avoid impact on end results.
- Increase flexibility: Changes during the migration project are effectively managed to ensure flexibility, while still meeting important deadlines
- Better use of resources: A dedicated Project Manager will enable the client to focus on their own jobs and utilise their core skills.

- Reduce costs: Migrating on-time saves time, resources, and money and the client should start to see the return on their investment earlier.
- As a part of the migration, standard PRINCE2 project controls will be implemented and followed including project planning, work-package scheduling, change control, communication planning, project reporting, escalation, risk management and mitigation. The project planning will document and agree the testing requirements and acceptance criteria for each component or work stream of the project.

2.3 Azure Cloud Management.

2.3.1 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 and 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).
- Cloud Compliance information and reporting.
- Continual service improvement for your cloud environment.
- Improved visibility for your cloud environment.
- Adaptive transformation to your cloud environment.
- Agile support and projects for your cloud environment.
- Service Governance for your cloud environment.
- Provide an effortless experience for users and customers for your cloud and hybrid estate.

2.3.2 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)

2.3.3 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).

2.3.4 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.

2.3.5 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.

2.4 Service delivery

Roc Azure cloud migration and management is delivered using the approach below:

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

2.4.2 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 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.

2.4.3 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.

2.4.4 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.

2.4.5 Service & Operational Tooling

Roc can 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.

2.4.6 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.

2.4.7 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

2.5 Service Level Agreements

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

2.5.1 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 • 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

2.5.2 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.

2.5.3 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 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.
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 security, 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.

2.6 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.