Service Definition: Microsoft Modern Work and Endpoint Management

Crown Commercial Services | G Cloud 15 framework

Contents

Document Information

Client name	G Cloud 15 Service Definition
Project name	Microsoft Modern Work and Endpoint 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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without the express written permission of Roc Technologies Limited and shall be held in safe custody.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

Microsoft 365 enables organisations of all sizes to deliver a comprehensive productivity suite to their users. It extends the capabilities of Office 365 by including Windows desktop licensing and the Enterprise Mobility + Security package, providing an integrated solution for productivity, security, and device management.

To summarise Roc's Microsoft 365 capability:

- Implementation of Microsoft 365 for green field developments.
- Migration of organisations to Microsoft 365 from on premises or alternate cloud providers.
- Tenancy to Tenancy migration and mergers within Microsoft 365.
- Microsoft 365 Security and Configuration auditing and best practice health checks for Cloud Compliance.
- Agile support and projects for your Cloud environment.
- Provision and cost optimisation of Microsoft 365 licenses.
- Roll out of mobile devices and endpoint management through Intune.
- Configuration of Endpoint onboarding through Autopilot.
- Configuration and rollout of MDM and MAM policies.
- Ongoing Management and Support for Microsoft 365 Tenancies and Service governance for your Cloud environment.
- User Helpdesk for Microsoft 365 and Office 365 applications.

2. Service Description

Roc's Microsoft 365 service combines expert professional support with managed services to ensure a seamless transition to the Microsoft cloud platform. We assist with migration, security implementation, and device management, while providing health checks and best-practice guidance. Our managed service underpins ongoing maintenance and support throughout your cloud journey. Roc are specialists in cloud hosting and Microsoft cloud technologies.

2.1 Microsoft 365 Features

Microsoft 365 is a suite of apps that help you stay connected and get things done.

- Microsoft 365 Apps - Unleash your best ideas, get things done, and stay connected on the go.
- Exchange Online - Connect, stay organised, and manage your time with business-class email, calendaring, and contacts all in one place.
- SharePoint Online - Share files, data, news, and resources. Customise your site to streamline your team's work. Collaborate effortlessly and securely with team members inside and outside your organisation, across PCs, Macs, and mobile devices.
- Microsoft Teams - Bring everyone together in one place to meet, chat, call, and collaborate.
- OneDrive - Save, access, edit, and share files and photos wherever you are.

2.2 Intune and Modern Device Management

Microsoft Endpoint Manager helps deliver the modern workplace and modern management to keep organisations data secure, both in the cloud and on-premises. Endpoint Manager includes the services and tools that are used to manage and monitor mobile devices, desktop computers, virtual machines and embedded devices.

Endpoint Manager combines familiar services, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, and respond and manage risk.

Endpoint Manager includes the following services:

- **Microsoft Intune** - Intune is a 100% cloud-based mobile device management (MDM) and mobile application management (MAM) provider for apps and devices. It allows control of features and settings on Android, Android Enterprise, iOS/iPadOS, macOS, and Windows 10/11 devices, including Windows Holographic. It integrates with other services, including Azure Entra ID, mobile threat defenders, ADMX templates, Win32 and custom LOB apps, and more.

With on-premises infrastructure, such as PKI or an Active Directory, the Intune connectors are also available:

The Intune Connector for Active Directory adds entries to on-premises Active Directory domain for computers that enrol using Windows Autopilot.

The Intune certificate connector processes certificate requests from devices that use certificates for authentication and S/MIME email encryption.

As part of Endpoint Manager, Intune can be used to create and check for compliance, and deploy apps, features, and settings to devices using the cloud.

Configuration Manager is an on-premises solution for managing desktops, servers, and laptops across internal networks or cloud environments. It can be cloud-enabled to integrate with Intune, Azure Entra ID, Microsoft Defender for Endpoint, and other cloud services. Configuration Manager supports deployment of applications, software updates, and operating systems, while enabling real-time compliance monitoring and remediation.

- Co-management - Co-management combines existing on-premises Configuration Manager investment with the cloud using Intune and other Microsoft 365 cloud services. As part of Endpoint Manager, co-management uses cloud features, including conditional access to ensure users and devices meet specific requirements before they are granted access to corporate resources.
- Desktop Analytics - Desktop Analytics is a cloud-based service that integrates with Configuration Manager. It provides insight and intelligence to make more informed decisions about the update readiness of Windows clients. The service combines data from the organisation with data aggregated from millions of devices connected to the Microsoft cloud. It provides information on security updates, apps, and devices within the organisation, and identifies compatibility issues with apps and drivers. The cloud-powered insights of Desktop Analytics within Endpoint Manager keep Windows 10* and 11 devices current. (*Where EUS is enabled).
- Windows Autopilot - Windows Autopilot sets up and pre-configures new devices, getting them ready for use. It is designed to simplify the lifecycle of Windows devices, for both IT and end users, from initial deployment through end of life. Autopilot can be used to preconfigure and automatically enrol devices in Intune.
- Azure Entra ID – Azure Entra ID is used by Endpoint Manager for identity of devices, users, groups, and multi-factor authentication (MFA). Azure Entra ID Premium, which may be an additional cost, has additional features to help protect devices, apps, and data, including dynamic groups, auto-enrolment, and conditional access.
- Endpoint Manager admin center - The admin center is a one-stop web site to create policies and manage your devices. It plugs-in other key device management services, including groups, security, conditional access, and reporting.

Roc offers a full inception to migration of Intune supported devices from legacy or third-party vendor solutions to enable organisations to reap the full benefit of their Microsoft licensing and

help reduce TCO. Roc can enrol and deploy devices in a hybrid or cloud-only configuration, removing Bloatware for new devices as part of an Autopilot deployment.

2.3 Microsoft 365 Security

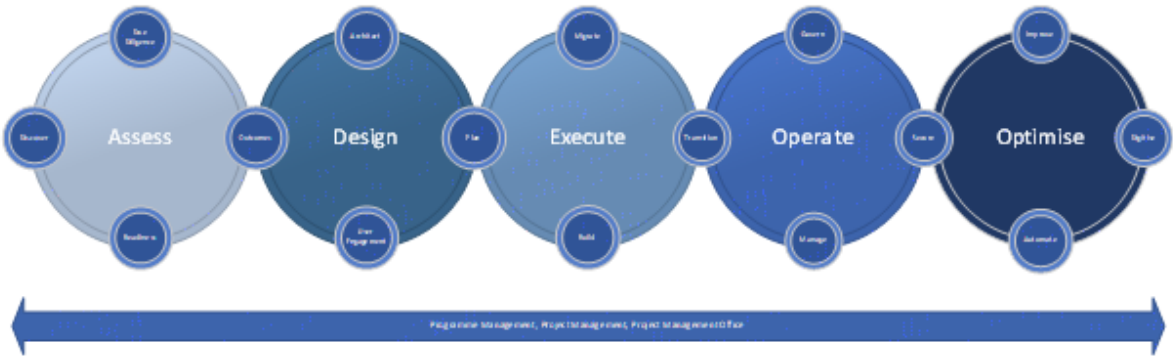
Roc is able to deploy, manage and maintain the full set of Microsoft 365 threat protection solutions.

- **Microsoft 365 Defender** - As threats become more complex and persistent, alerts increase, and security teams are overwhelmed. Microsoft 365 Defender, part of Microsoft's XDR solution, leverages the Microsoft 365 security portfolio to automatically analyse threat data across domains, building a complete picture of each attack in a single dashboard. With this breadth and depth of clarity, defenders can now focus on critical threats and hunt for sophisticated breaches, trusting that the powerful automation in Microsoft 365 Defender detects and stops attacks anywhere in the kill chain and returns the organisation to a secure state.
- **Microsoft Defender for Endpoint** - Microsoft Defender for Endpoint delivers industry-leading endpoint security for Windows, macOS, Linux, Android, iOS, and network devices and helps to rapidly stop attacks, scale your security resources, and evolve your defences. It's delivered at cloud scale, with built-in AI that reasons over the industry's broadest threat intelligence. Our comprehensive solution enables discovery of all endpoints and even network devices, such as routers, in your environment. It offers vulnerability management, endpoint protection, endpoint detection and response (EDR), mobile threat defence, and managed hunting all in a single, unified platform.
- **Microsoft Defender for Office 365** - Protect all of Office 365 against advanced threats like business email compromise and credential phishing. Automatically investigate and remediate attacks.
- **Microsoft Defender for Identity** - Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organisation.

2.4 Service Delivery

2.4.1 Professional Services

Roc offers packaged services for deploying, maintaining and supporting Microsoft 365 services. Using our service delivery model as a framework allows our skilled and certified professional services teams to carry out a wide range of services related to Microsoft 365.



Roc has many years of experience in deploying Microsoft 365 both in green field deployments or migrating customers from legacy on-premises solutions to the Microsoft Cloud providing an effortless experience for users and customers for your Cloud and hybrid estate. Roc has also undertaken tenant to tenant migrations to support business mergers and acquisitions. For existing deployments we are able to provide health checks to verify security and best practice configuration and ensure cloud compliance.

2.4.2 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.

2.4.3 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 is also able to provide SC and DV cleared resources. Roc is a long-standing Microsoft partner and also holds the Modern Work Solutions designation.

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

2.4.4 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.

2.4.5 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.

2.4.6 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.

2.4.7 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.

2.4.8 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.

Please refer to section Service Level Agreements for further information.

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: -	15m	30m	4h

	• Complete network failure • Simultaneous failure of resilient WAN links • Core application/service down			
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 representing Additional Service Points

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.