Service Definition: Managed Services

Crown Commercial Services | G Cloud 15 framework

Contents

1. Service Summary 5
1.1 Overview 5
1.2 Services Summary 6
2. Service Description 8
2.1 Services which can be included 8
2.2 Proactive Cloud Support 12
2.3 Accreditations & Vetting 15
2.4 Support Mechanism 16
2.5 Account Governance & Collaboration 16
2.6 Support Model & Agreements 17
2.7 Service & Operational Tooling 18
2.8 Change Management 18
2.9 Service Level Agreements 20
2.9.1 Hours of Cover 21
2.9.2 Incident Management 21
2.9.3 Change Management 23
2.9.4 SLA Terms 23
2.10 Service Delivery Management 24
2.11 Continuous Improvement 26
3. Service Pricing 28
3.1 Onboarding Fees 28
4. Terms and Conditions 31

Document Information

Client name	G Cloud 15 Service Definition
Project name	Managed Services
Document author(s)	David Jordan, 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.

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

1.1 Overview

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.

The illustration below provides a high-level overview of the Managed Services that Roc can deliver. This is underpinned by shared resource pools of technical expertise and aligned, named stakeholders who provide the oversight and assurance for our services.

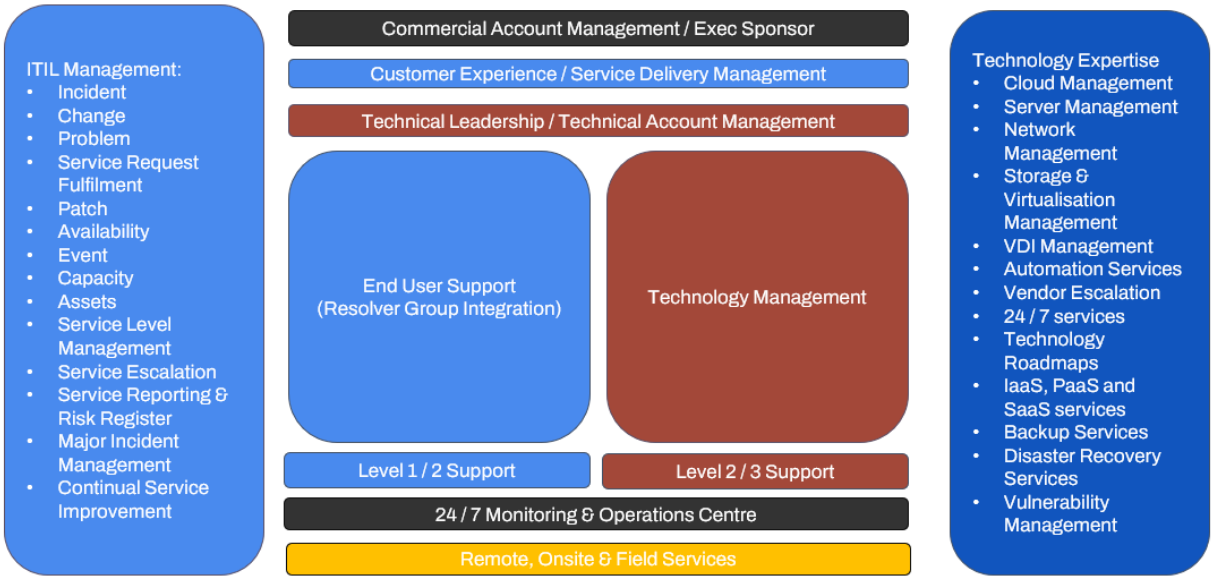

Figure 1 – Roc Managed Service Capability

Roc's key premise is to deliver an effortless client experience in all environments, from local government and local authority organisations through to those that are considered secure and highly regulated such as within Government, NHS, Nuclear, and Ministry of Defence sectors. Our technical expertise, experience, and security accreditations ensure we adhere to security compliance of all levels.

We use a combination of dedicated resources and shared support to ensure that you have access to known individuals who understand your environment and your business as well as a pool of highly skilled engineers who can support them as needed during any peaks.

We apply the following principles to ensure that the focus is on business outcomes and deliverable solutions:

- All solutions are based on achieving business outcomes as priority with technology following on.
- End to end ownership and management of solutions.

- Drive customer success and analytics.
- Strategy of single customer engagement platform (ServiceNow) that delivers scalable and repeatable, high value service.
- Customer access choice with option of Self Service through as much of the customer Life Cycle as possible.
- Far fewer customer handoffs and reduce the need to engage support.
- Setting the right levels of expectations and hitting those consistently.
- Driving customer loyalty by reducing effort in every part of the engagement.

1.2 Services Summary

The main elements of a Roc proposed core Managed Service solution are described below.

- Remotely delivered managed service (onsite managed services options are available) for proactive service related to customer Cloud platforms.
- A Service Delivery Manager (SDM) to ensure the service is customer focussed and focussed on excellent service delivery. To attend regular service reviews where past service status is discussed.
- Production of a Continual Service Improvement Plan (CSIP) and Technical Service Improvement Plan (TSIP) to ensure the service delivered remain current and continues to match expectations throughout the contract term.
- Continual Service Improvement for your Cloud environment.
- A trusted advisor / technical lead included to provide thought leadership, proactive technology roadmaps and heatmap artefacts.
- The technical lead will provide overall technical ownership and be responsible for driving lifecycle management, technology plans and the delivery of an exceptional end user experience.
- Regular service reports providing service level, ITIL and cost visibility. Service reviews to proactively engage on the Managed service. Both reporting and service review can be delivered monthly or quarterly, either onsite or remotely.
- Access to Roc's Professional Services team that deliver transformational projects for our customers using world class technologies.
- 24x7x365 monitoring, management and support of the client's Cloud and Hybrid estates.
- Backup and DR (Disaster Recovery) as a Service delivered if required. DR, backup and recovery tests included.
- Patching as a service for key services and technology components.
- Lifecycle, Vulnerability and threat management for software and hardware. Including the identification and remediation of software risks, through patching and upgrades.

- Cloud native network Managed Services, utilising Artificial Intelligence and machine learning.
- Any service proposal will allow for potential growth or reduction in numbers expressed as a +/- percentage.
- Cost Optimisation, right-sizing and control for your Cloud environments.
- Cloud compliance information and reporting.
- Service governance for your Cloud environment.t
- Business value and outcomes based delivering Cloud success.
- The Roc Managed Service will be responsible for ongoing remote management and monitoring of the Cloud platforms.

Our core practices include Networking, Cloud, Cybersecurity and Data and AI, with all practices underpinned by our 24/7/365 in-house Managed Services capability. To support these practices, we have strategic partnerships with world-leading technology partners including HPE, Microsoft, Google, Juniper Networks, CATO, Palo Alto, Netcall and Fortinet.

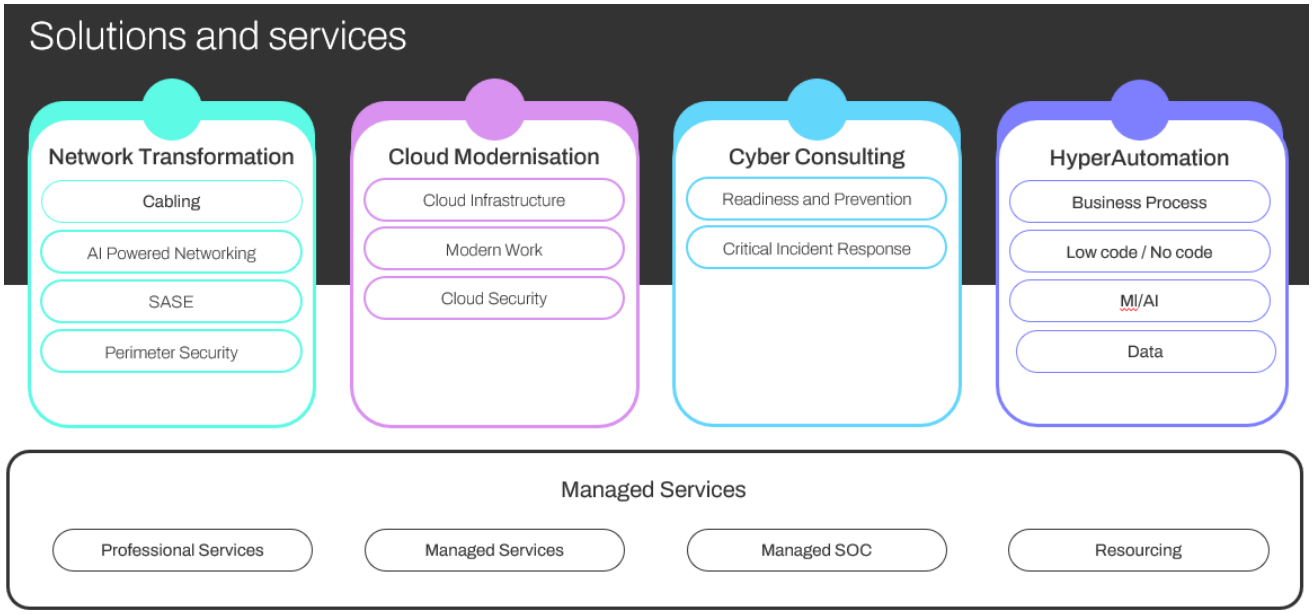

Figure 2: Roc Technologies' Services Portfolio

Roc holds some of the UK's most stringent data and security accreditations, including universal SC to DV clearance within our technical teams. Over 50% of our technical team members holding these clearance levels.

2. Service Description

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

2.1 Services which can be included

- **Service Catalogue**: Roc will implement a service catalogue defining the services, software and physical assets in scope. This information will be gathered during the service transition and held in our ITSM platform, ServiceNow. This information will be shared with the customer, with this information being part of service reporting collateral provided. During the service lifetime, updates will be performed the catalogue aligning to any installations, moves, changes and additions that have taken place.
- **Contact Management.** Providing telephone, email, chat and portal functions via Roc's ITSM ServiceNow toolset. Roc provides a 24/7 Managed Services Operations Centre (further details provided below) that enables incidents and requests to be logged via telephone, email, and portal functions that is accessible via Roc's ITSM toolset. Approved Technical Points of Contact can be provided with a management level view of tickets, whilst end users and IT staff have the ability to log and provide updates to tickets.
- **Service Desk.** Roc can operate a 24x7x365 first, second and third level Service Desk located from our two operations centres. The Service Desk analysts are overseen by a team of Supervisors and an out of hours Duty Manager who are committed to deliver a high level, customer focused managed service to our customers. Roc underpins its IT Service Management with ServiceNow. ServiceNow is used to deliver a number of ITIL based disciplines, including but not limited to, Incident, Change, Problem Management and so on.
- **Response & Escalation Service Levels.** Providing effective and timely responses to Incidents is key. Moreover, ensuring these are measured and escalations (if needed) appropriately. The table below outlines these mechanisms that will underpin the service. Roc's adherence to these will be governed and reported upon by the Roc Service Delivery Manager (SDM). An Escalations Matrix is pre-agreed between Roc and the Customer, providing a tiered escalation path on both sides. This matrix is detailed within the Service Delivery Plan and covers the escalations path for both Commercial and Service-related issues.
- **Incident Management**. Incident Management is a core process for the Service Desk to ensure that any disruption to service is accurately recorded and managed through to service restoration. Incidents are prioritised and allocated by impact and urgency,

Supervisors oversee the day-to-day management of all calls alongside a culture of best practice and ownership of tasks throughout the team.

- Problem Management. The Roc Problem Management process aims to proactively prevent the re-occurrence of incidents, problems and errors within the IT infrastructure, in order to reduce the impact of these occurrences. It incorporates root cause analysis and investigation, development of workarounds where possible, and the implementation of fixes in alignment with Change, Release and Deployment processes.
- Patch and Vulnerability Management defined by the patching policies. Roc will apply a schedule for patching and vulnerability management. This schedule will be agreed with the client as part of the service transition and can be flexed/changed upon agreement by all parties. It should be noted, this doesn't preclude out of band patching taking place, when a critical vulnerability or bug is identified. For these scenarios, an exceptional patching event and case will take place. Patching and vulnerabilities will be identified through automated scans, then assessed, tested and deployed. This will cover the end-to-end lifecycle of software, hardware and applications. Roc's patching cycle is aligned to vendor best practices and follows a simple, but stringent framework to IDENTIFY-ASSESS-TEST-DEPLOY the relevant patch updates.
- Change Management. The Change Management process is initiated by the Service Desk when a request for change is received from the customer or during an incident if an emergency change is required to restore service. The Service Desk are responsible for overseeing the information gathering stage and identifying the type of change that will be undertaken, they will include a full test plan, outline of tasks and rollback plan. Details of any likely or potential impact will be documented in the change and then the Roc CAB will review and approve/decline changes after considering the business and technical requirements, impact and urgency of the work. Changes are sent to the customer for approval. Change are broken down into different categories of Emergency, Major, Minor and Standard. Each with associated processes for creation, approval and implementation. The process includes appropriate timescales based on the priority and category of change.
- Lifecycle Management. As part of this service Roc would include information in the service reports that will highlight all the hardware and software in scope for this service. Where possible Roc will include a table highlighting the lifecycle of these assets.
- Monitoring. Roc will continue to use its NinjaOne Cloud 24x7x365 monitoring for server and network assets. The NinjaOne monitoring coverage thresholds for critical system metrics and automatic alert generation (in event of exceeding the thresholds), allows Roc to be alerted to issues reported by the monitoring application.

- **Event Management**. Roc operates a comprehensive managed service platform that includes monitoring and alerting for numerous aspects of a virtual and physical IT estate. Critical monitoring alerts are automatically reported directly to the Roc Service Desk and are logged, investigated, and reported on as is appropriate to the severity of the alert. Where investigation of a monitoring alert indicates the existence of an Incident or Problem, the Service Desk will manage the incident in accordance with Roc's processes. Roc's monitoring toolsets, underpinned by process, also allow for the sequencing of events to ensure personnel really understand what events are important to the customer.
- **Knowledge Management**. The purpose of Knowledge Management is to gather, analyse, store and share knowledge and information within Roc and the function that support our customer's Managed Services. Roc fully understands that the ability to deliver a quality service is impacted by the ability of those supporting that service to respond to situations based on their "knowledge" of the situation, the options, and the consequences of decisions.
- **Availability Management**. The client service can be managed to optimise the availability and reliability of services, the supporting infrastructure, and resources, in order to ensure that the overall requirements for services can be met. The scope of availability and risk management will entail activities to ensure preventative and corrective maintenance is undertaken. The first action will be to provide basic availability reports as part of the service review.
- **Capacity Management**. The client's services will be managed to optimise the capacity of services in order to ensure that the overall requirements for services can be met. Capacity management is the function and process whereby IT Services are managed to match the supply of IT resources against the demands from the end user. The scope of capacity management will entail activities to ensure preventative and corrective maintenance is undertaken, with the aim being to identify longer term trends and capacity information.
- **Service Requests**. Service Requests logged with the Roc Service Desk will be assigned to the appropriate team for action in line with the customer requirement. The Roc Request Fulfilment process takes account of the service scope and request parameters to ensure that tasks are fulfilled promptly. Out of scope requests are promptly escalated to the appropriate Service Delivery Manager or Account Manager for consideration and discussion with the customer.
- **Technical Support**. Roc would provide subject matter expertise for the in-scope technologies. This is underpinned by the vendor accreditations Roc has attained for vendors such as Microsoft, Citrix, Juniper, HPE, Aruba, VMWare, Cisco, Fortinet and Palo Alto. Roc will also, where required, leverage expertise from its Professional Services teams to enhance support and work with key vendors to escalate specific problems.

- **Operational Activities.** Operational Activities are managed through the Service Desk and can consist of any operational task or check that has to occur at regular intervals (for example batch jobs, system checks, system diagnosis and daily administration.). The relevant Operational Activities for the client's Managed Service proposition will be discussed and detail and defined as part of the service transition process. These activities do vary between technologies and ensuring these are right for the service is critical to ensuring a comprehensive service is delivered. Moreover, Roc strives to automate these activities where possible through its monitoring toolsets but will also utilise administrator consoles for the relevant technologies.
- **Third Party Management (Vendor Escalations**). Roc's partnerships span multiple vendors and technologies each specialising in solutions that can support your business needs. Roc would utilise its Partner status with vendor to deliver seamless service. Roc work closely to ensure our customers benefit from the most appropriate solutions and provision across our managed service. The Service Desk can facilitate fault reporting, escalations and communications with other vendor partners to act as a single point of contact for all IT support services. Utilising our ITSM and in-house tools to track requirements, status, updates and service targets Roc can integrate across multiple platforms with multiple partners.
- **Service Delivery Management**. The client would have an aligned Service Delivery Manager (SDM) who will be responsible for managing the overall service and will provide a management framework to ensure Service Levels are achieved and to deliver continuous improvements in service quality aligned to business requirements. This will be achieved through a continuous cycle of agreeing, monitoring, reporting, and reviewing service achievements and through instigating actions to eradicate any unacceptable levels of service. The SDM function will incorporate the existing service to ensure a holistic approach and comprehensive delivery approach.
- **Service Level Management**. Roc will provide Service Level Management for defined response, resolution and availability SLAs. Typical SLAs are outlined below. Our performance against these SLAs will be reported and discussed during the scheduled service reviews and reports.
- **Service Reviews & Reporting**. Roc would incorporate monthly or quarterly service reports provided via the SDM. Giving clients improved Visibility for your Cloud environment. This would be underpinned by either monthly or quarterly service reviews also.
- **Knowledge Management**. Roc place strong emphasis on the continuous development of the customer and our teams' expertise, recognising that the dynamic nature of technology demands ongoing learning and upskilling. Ensuring our delivery teams are up to date with technology changes, we work with our

strategic vendors, including Microsoft, Juniper, Fortinet, HPE Aruba, and Dell vendor to ensure we're fully trained on all the key technologies and products.

- **Backup as a service**. Roc would work with its existing backup service partner to deliver a cloud hosted backup solution for the clients local and cloud hosted data. The cloud-based consumption model allows the client to flex the service based on current backup needs, with cost based on the no of users and the volume of data subject to a minimum charge. Roc would look to implement operational activities and proactive monitoring steps to ensure optimal backup performance and availability. The backup schedules, types and retentions would be subject to due diligence, Roc would monitor backup failures, successes, and time spans as part of the service, with alerts raised as tickets and progressed as part of its standard service processes.
- **Digital transformation**. Roc has extensive experience in the field of Business Process Management that runs from process discovery and communication through optimisation and on to digitisation and automation. Our services have been employed on a wide range of process related projects from major business transformation and change programmes to enterprise-wide software implementations to merger and acquisition.
- **End User Device (UD) Management**- IT remote support for the User devices, including patching and upgrade management using Intune. Roc has worked with many customers across the full lifecycle of services. Roc can provide a fully managed end user device managed service, as well as the project services to design, implement and transition these.
- **Cloud and Technology Management** – Roc would look to provide Proactive cloud advice, providing adaptive transformation to your Cloud environment through Agile support and projects. As part of the cloud management Roc would look to provide an effortless experience for users and customers for your Cloud and hybrid estate. Our technology management includes providing insights, Role Based Access Controls and orchestration of Cloud tasks.
- **Cost and Security Optimisation**. We will provide visibility and trend information, for the customer to make informed financial management decisions. This includes right-sizing, auto-scaling and threat mitigation recommendations. This optimisation is underpinned by toolsets such as Azure Advisor and SecureScore.

2.2 Proactive Cloud Support

We offer end-to-end management of Microsoft 365 and Azure tenancies, encompassing user provisioning, licensing, security configurations, and application support. Our approach guarantees a client's cloud environment would remain optimally configured, be secure, and

compliant with the latest standards. We also oversee Azure tenancies, ensuring that resources are efficiently utilised, costs are optimised, and the infrastructure is resilient.

Roc's principal offerings for Public Cloud centre on Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), however within its role as a Managed Service Provider a number of Software-as-a-Service capabilities have also been developed too. IaaS is principally provided through Microsoft Azure for highly secure services. PaaS is offered for solutions such as Low-code, firewalls, and SQL Server, whilst a number of SaaS solutions are commonplace such as O365, M365, web and email filtering. Roc currently manage and maintain Azure for customers across the Nuclear, Government, Finance and recruitment sectors.

Roc's monitoring and detection mechanisms will address issues in real-time. This includes monitoring Exchange Online mail flow, SharePoint site performance, Teams availability, and telephony services. Our support team will provide remote assistance for desktop applications, including accessibility tools for users with diverse needs, ensuring users receive timely resolutions to their queries and technical issues. When managing 365 and Cloud technologies, a holistic approach to managing these services is vital, with the following key disciplines applied to each technology component:

Figure 3 – Cloud Management Principles

A vital aspect of technology management is maintaining a comprehensive Knowledgebase and knowledge sharing process. At Roc, this is underpinned by regular knowledge transfer sessions, our ServiceNow platform and integration with customer data repositories also.

Roc offer an innovative service called SCOUT, which is an AI-powered platform specifically designed to help our customers optimise cost, security, governance and resource management for both Azure and Microsoft 365 that will be included as part of this managed service. This FinOps service will provide detailed views of Microsoft Cloud consumption and is included in our core offering, with the key activities involved outlined below:

- Roc's Solution Architecture team will create a proposal to onboard you into our Premium FinOps Managed Service Platform
- Utilising Best of Breed tooling, including ServiceNow, SCOUT, and Microsoft platforms, Roc will continually assess and proactively manage your Microsoft environment to ensure optimum value and utilisation
- Roc's Service Management team will present changes, cost savings, and improvements on Monthly service reviews.

Key Features of SCOUT:

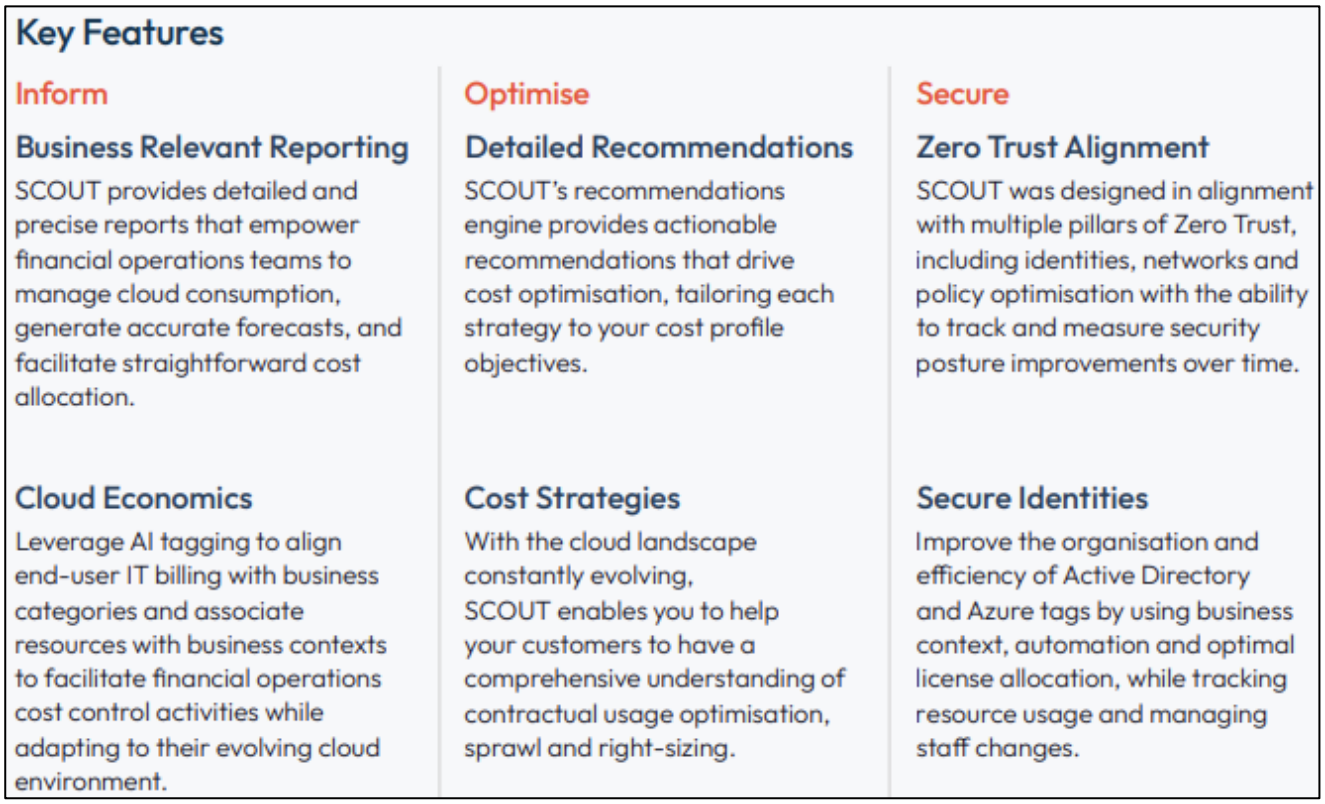

Figure 4 – Cloud Assessment Benefits

As part of the SCOUT service, we will monitor and report on Microsoft Secure Score and Azure Secure Score to assess the security of Microsoft 365 and Azure environments. These assessments will provide actionable insights to improve the overall security of Microsoft services, including Exchange Online, SharePoint Online, and Microsoft 365 apps as well as Azure resources and workloads. If vulnerabilities are identified, they will be categorised and reported on as part of the service review. The report will be delivered with suggested remediation activities.

We build our Cloud Management services on the premise of delivering proactive services that are summarised in the illustration below:

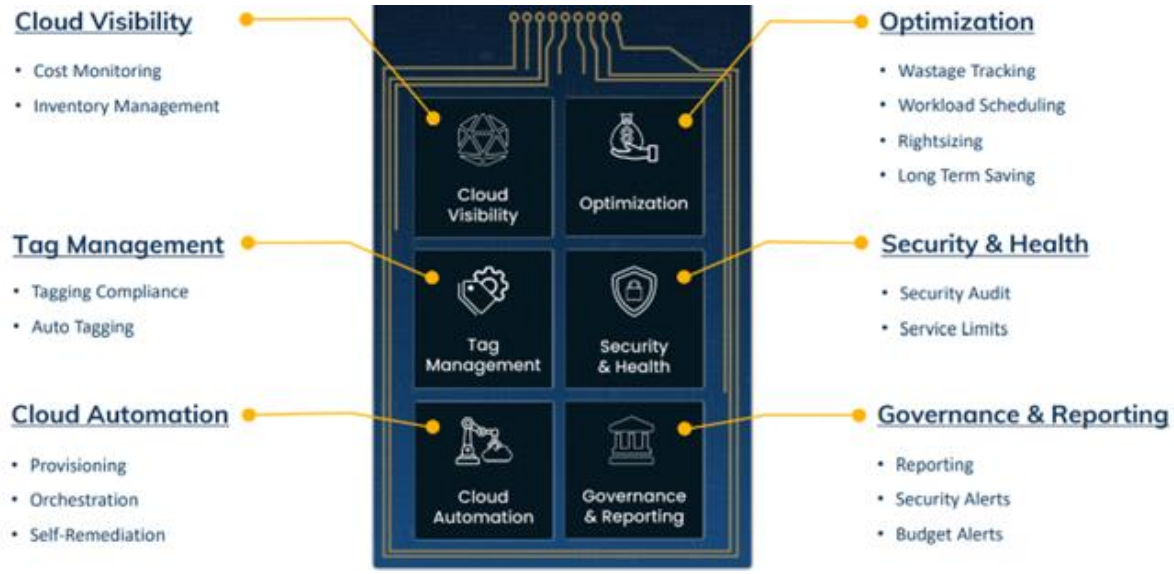

Figure 5 – Cloud Management Methodology

The services within this document are designed to operate as a first line service desk, second or third level resolver groups.

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.

2.3 Accreditations & Vetting

Roc's Security 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, security and other standards. We hold ISO 20000, ISO 27001, ISO 9001, ISO 45001 and ISO 14001. Additionally, we hold Cyber Essentials Plus for our internal systems and delivery of Cloud Managed Services.

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.

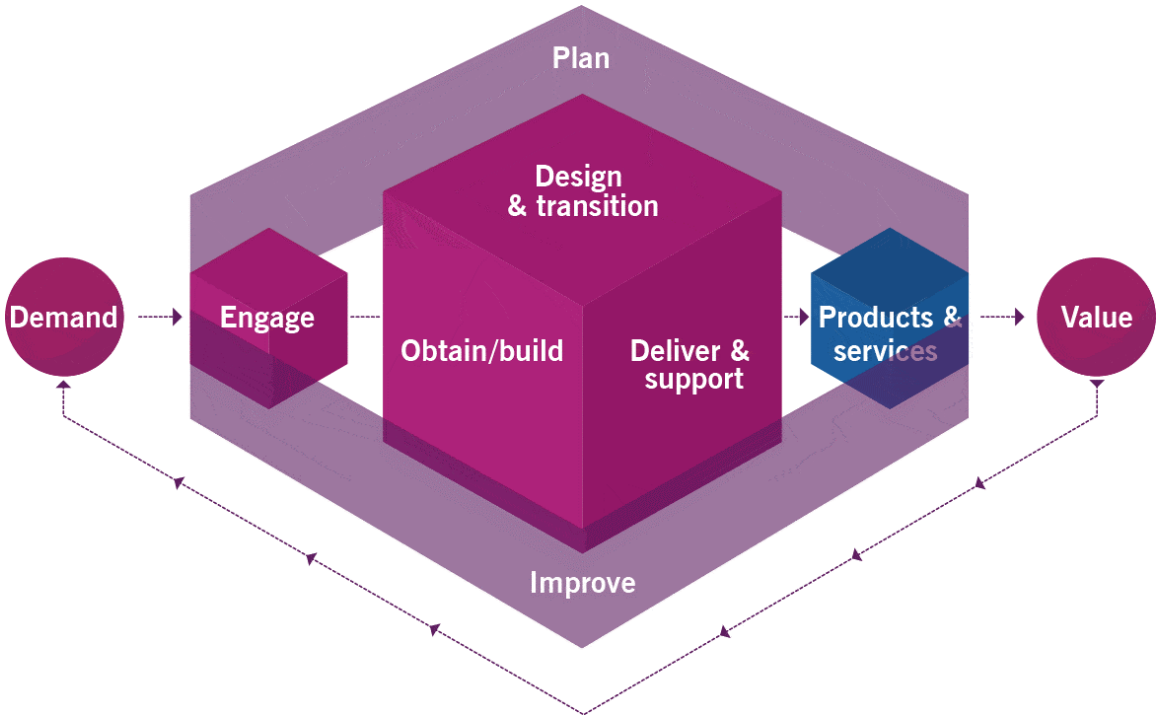

Figure 6 – ITIL Framework

Roc can offer Managed Services and Consultancy to prospective Clients. Roc considers security of our own and our customers' systems to be an imperative. We hold the ISO27001 standard for Information Security Management Systems (ISMS) and for some of our existing managed service customers we require the highest level of security accreditations to meet their security and controls, these include CESG (the UK Government's National Technical Authority for Information Assurance) and the National Cyber Security Centre (NCSC). Roc also provides managed services for several customers within secure and sensitive industries.

2.4 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.

2.5 Account Governance & Collaboration

Roc has recognised the requirement for an account governance structure across the key disciplines of technology and innovation, Service and Continual Service Improvement Planning (CSIP), Commercial, Operations (Capacity, Problem, Incident, Change Delivery, Security and Risk). This can be flexed to match the requirements of customers and by default Roc propose service governance delivered by the following key roles:

- Account Manager.
- Service Delivery Manager.
- Technical Lead / Design Authority.
- Executive Sponsor.

The relationship with client's will be managed by two key stakeholders within Roc, the Account Manager, and the Service Delivery Manager (SDM). The Account Manager is responsible for the ongoing commercial relationship with the customer and the SDM is responsible for the delivery of service and service performance. Regular communications between all three parties, with a scheduled formal service review and commercial meetings where expectations would be set. Monitoring and measuring would be performed via a customer relationship survey (CSAT) and reviewed regularly both with client's and internally within Roc.

Aligned to the above, a named Technical Lead will be the customer's Technical Authority and trusted advisor for the account. The person appointed would be a highly experienced technical resource who has expert Network, O365, Cloud and virtualisation knowledge to call on. This role will provide defined artefacts for the customer such as lifecycle heatmaps, technology roadmap, technology forums, sector and market knowledge and vendor engagement.

Roc's 'One team' approach is the key to successful engagement, ensuring that service delivery engenders a collaborative approach through the delivery of a tailored IT solution. This approach will include the development of a comprehensive IT strategy for customers. Below are some key concepts that Roc will adopt with customers to enable us to work collaboratively to deliver a successful IT strategy:

- Aligned vendor, customer and Roc interfaces.
- Defined cadence, checkpoints, workshops and proactive sessions with the vendors and the customer.
- Underpinned by Roc and vendor Subject Matter Experts.
- Covering technical, service, commercial and strategic deliverables.
- Providing Insurance and Defence skills and experience.

This 'one-team' approach ensures the customer benefits from an effective and efficient delivery model which ensures that the organisational needs and objectives are met.

2.6 Support Model & 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.

Our 24x7 UK based operations centre delivers comprehensive support for Microsoft Azure Infrastructure and Microsoft 365, ensuring secure, efficient, and resilient cloud operations for our clients. All requests and incidents are logged through our dedicated support portal, which provides real-time visibility of progress, service-level tracking, and direct communication with our technical specialists.

Support is delivered through a tiered structure:

- 1st Line Support handles initial queries, basic troubleshooting, and common administrative tasks, ensuring quick resolution for routine issues.
- 2nd Line Support addresses more complex technical incidents, configuration changes, and escalations from 1st Line.
- 3rd Line Support manages advanced troubleshooting, platform-level changes, architecture reviews, and liaison with Microsoft for critical issues.

Access to client environments is strictly controlled using Role-Based Access Control (RBAC), ensuring that each team member only has the permissions necessary to fulfil their responsibilities. Privileged Account Management (PAM) is used to provide just-in-time elevated access, with all administrative activity logged and audited for compliance and security.

2.7 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.

2.8 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.

Roc views change management as a critical process for itself and its customers. As a result, Roc has developed a mature change management approach that can integrate with customers easily. Roc can provide customers with a fully functional Change process of its own or integrate tightly with an existing customer change management process.
Effective implementation minimises operational risks while using standard procedures and methods. Ensuring less disruption of IT services across an organisation or department is clearly valuable but so is decreasing the risk associated with change.

The decision to update and change systems is driven by the desire to improve services and products or reduce risk. ITIL change management ensures introduced changes are effective,

with a keen focus on customer satisfaction. It also ensures that business needs are catered for, with all changes to documents recorded.

Change management is a program that addresses the scope and extent of any changes. This includes:

- Service assets such as physical servers and storage.
- Virtual or cloud storage and servers.
- Third-party software provided by external providers.

A methodical approach is essential to change management to ensure that nothing is missed and that risks are foreseen.

Under ITIL change management, there are three categories of change to manage the process:

- Standard change is easy to implement, low risk, and doesn't require senior management approval prior to implementation.
- Normal change requires approval as the potential risks to service delivery need assessing beforehand.
- Emergency change responds to an emergency situation and includes senior managers. The workflow for these changes is the same as that identified for a normal change, but the urgency drives the process.

Roc believes that to achieve a positive outcome for a change request it is essential that the change is fully defined. The list below defines the requirements for the change management process:

- Requests for Change (RFC) can be the result of Incidents, problems and availability issues or Service request from Roc Customers.
- Changes are categorised as Emergency, Normal and Standard (pre-approved).
- Each change will be assigned a unique reference number.
- Technical and operational assessments will be carried out for all changes.
- The implementation of each change should be managed through from request submission to change incident review.
- Schedule duration of the Change must include back-out timing, ensuring adequate time should the "Back out plan" be invoked.
- If the change is not successful, then the agreed back out plan will be implemented.
- A clear record of the change's progress should be available.

Roc's standard practice is to hold a periodic Change Advisory Board (CAB) to approve or reject changes. Written authorisation for the change will always be required; authorisation by email will be accepted. These will be filed on Roc's ITSM to support the RFC. When a change is implemented, any relevant alterations to Design and Configuration documents should be made (QRG).

2.9 Service Level Agreements

Service Levels and Escalation

- Incident Response and Resolution: Defined response and resolution times for Priority 1–4 incidents, including clear definitions for “business hours,” “clock stop,” and escalation protocols.
- Escalation and Dispute Resolution: Documented escalation paths for both technical and commercial issues, named escalation contacts, dispute resolution procedures, and timelines before financial penalties apply.

Incident Response and Resolution:
Roc Technologies’ service will provide clear and proven Incident service levels, with associated escalations management and dispute resolution.
For our Incident Response and Resolution service levels, we are pleased to offer both and further add value through priority-based service levels, including 24x7 cover for P1 incidents.
We define Response and Resolution as follows:

- Incident Response – Measured from the timestamp when the Incident record is created in our IT Service Management system, to the timestamp when the case is picked up by the engineer
- Incident Resolution – Measured from the timestamp when the Incident record is created in our IT Service Management system, to the timestamp when the record status is updated as resolved by our engineer

Should we need to pause the service level timer (“clock stop”), this will be due to a dependency on actions outside of our control. For example, if we are waiting on more information from a user or your IT.

Roc’s defined Major Incident Management process runs 24x7, with rapid mobilisation of technical resources, assigned Major Incident Manager and defined technical escalation.

We ensure consistent service level adherence, responsiveness and escalation procedures by aligning with ITIL4 best practice and automating our ways of working. Within ITIL4, there are 4 dimensions that come together to deliver services, which are the processes, people, toolset, and suppliers. We combine all of these together to ensure predictable, consistent and reliable outcomes.

We adopt where possible the processes and procedures defined within our enterprise-grade IT Service Management (“ITSM”) system, ServiceNow, so that they're standardised, out-of-the-box configurations, and systems-driven, with pre-defined inputs, outputs, triggers and activities, including timers for when:

- Activities need to be completed to meet our Service Level commitments.
- Escalations are needed to for higher levels of technical and management engagement.
- Communications are needed, to ensure affected parties and stakeholders are kept informed of progress.

Because our ways of working are automated in our ITSM system, we also have a highly effective way of conducting Continual Improvement, as any improvements identified can be quickly and effectively applied at the system level, further enhancing and ensuring consistent service availability, responsiveness and escalations.

Escalation and Dispute Resolution
Technical issues will by escalated by following our proven and reliable, automated paths that are configured in our ITSM system. This ensures management notifications and interventions are triggered as more of the service level timers are progressed, to engage additional and more advanced engineers to resolve the issue within the service level timeframes.

The service level timers also trigger progressively higher levels of management focus and engagement with you, to keep you informed and involved as an escalation progresses. This management escalation is captured in an Escalations Matrix, which will be defined with you during Service Transition to ensure the correct peer-to-peer relationships are captured. The following table provides an example Escalations Matrix:

	Roc Technologies	Customer
Tier 1	MSOC Team Leader	Operations Manager
Tier 2	Service Delivery Manager	Service Owner
Tier 3	Head of Operations	Service Owner
Tier 4	Head of Customer Experience	IT Director
Tier 5	Services Director	IT Director

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

2.9.1 Hours of Cover

Roc's Managed Cloud Services are offered based upon two standard SLA's:

- 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

2.9.2 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	30m	1h	4h

	a supported system. No acceptable workaround available. Examples include: - • 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	8h
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

2.9.3 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

2.9.4 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.

2.10 Service Delivery Management

To ensure transparency, Roc would establish a robust reporting and access framework. The cornerstone of this framework is the Service Delivery Manager (SDM) who would play a pivotal role in monitoring the account and providing regular service reviews. Held monthly or quarterly, the SDM would engage with the customers IT staff and key stakeholders to conduct in-depth service reviews. These reviews serve as a platform for open communication, where key performance indicators (KPIs), service levels, and adherence to required standards can be thoroughly examined.

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 places great emphasis on regular, continuous conversations and cadence with our customers. Below is the typical cadence we put in place with customers when delivering Cloud services:

- Monthly Service Reviews: Regular service review meetings held remotely and/or on-site to assess performance and issues.
- Agreed Metrics: Monitoring of key service metrics including ticket volumes, resolution rates, and customer satisfaction levels.

- **Change Management**: Clearly defined change management procedures, including methods for approval, risk assessments, documentation, and version control.
- **Proposals for Improvement**: Ongoing recommendations for cost savings, operational efficiencies, and security enhancements.

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

- Incident management including a summary of incidents raised, open, category, and priority.
- Roc's performance against the service levels in the relevant month and service measures.
- Quantitative and qualitative service reports/graphs covering trends and areas for education and improvement.
- Problem management including a summary of problems raised, open, category, and status.
- Service request fulfilment including a summary of requests raised, Status, and the category.
- Change management including a summary of changes raised, failed and closed in the period, category, priority, etc.
- Capacity management including a summary of capacity management status, trends, and details of any capacity issues in the period.
- Availability management including a summary of availability management status and details of any availability issues in the period.
- Patch release and deployment management including a summary of releases in the period and compliance.
- Operations management activities and issues identified in the period.
- Updates to agreed MIR remedial actions.
- Third party performance against their committed service levels.
- Asset summary, lifecycle information and support advisories (for example end-of-life statement and upgrade recommendations).
- Cloud optimisation and security reporting based on information from our SCOUT assessment toolset, Azure and M365, identifying efficiencies and gains.
- General observations and recommendations.
- Service improvement plan including an update of improvement actions and progress made in the period.
- Overall customer and user satisfaction measures, including CSAT surveys.
- Relevant progress reports on projects and other professional service undertakings.
- Endpoint status, health, performance and anti-malware status of devices.
- User Access Reviews – reports on privileged access and changes (subject to agreeing the toolset required to deliver this information).

The illustration below shows reporting information provided to an existing Roc customer. This example includes recommended actions to increase the customer's 'Secure Score'.

Rank	Recommended action	Score impact	Points achieved
1	Ensure multifactor authentication is enabled for all users in administrative roles	+0.71%	0/10
17	Stop clear text credentials exposure	+0.35%	0/5
20	Protect and manage local admin passwords with Microsoft LAPS	+0.35%	0/5
26	Ensure Sign-in frequency is enabled and browser sessions are not persistent for	+0.35%	0/5
79	Designate more than one global admin	+0.07%	0/1

Figure 7 – Example Security Recommendations

2.11 Continuous Improvement

Roc places high value on the delivery of Continuous Service Improvement (CSI) and Customer Experience to drive business value and efficiency. 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.

Roc strictly adheres to a principle of CSI. It is responsible for managing improvements to the Roc services. The performance of those services is continually measured, and improvements made. Roc's CSI lifecycle approach is based on the following key objectives and scope of process:

- Quantify and track benefit provided to the customer of improvements to processes and services including the delivery of services at levels beyond the agreed SLAs and KPIs.
- Review, analyse, priorities and make recommendations on improvements that can be made with-in the services provided by Roc.
- Identify and implement specific activities to ensure SLA achievement and prevent reoccurring failures identified by the problem management process.
- Implement improvements approved by the customer within agreed timescales.
- Review and improve the effectiveness of the CSI process itself.

Roc utilises industry best practise via the Deming Cycle (Plan, Do, Check, Act). This approach ensures the CSI process delivers to the key values it intends:

- Improvements.
- Benefits.

- Return on investment.
- Value of investment.

The Service Delivery Manager and Technical Lead (from the Solutions Architecture Team) would help facilitate this process and the Continual Service Improvement Plan (CSIP) used to drive and track the progress. The CSIP will underpin service value and development. The account team – Account Manager and Service Delivery Manager will be the key drivers of the CSIP.

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, 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.

The seamless transition of service into the Roc Managed Service is critical. Ensuring there is no impact to users, and the new service provides skilled representatives in a timely and efficient manner is of paramount importance. All transitions will be planned and communicated within a project plan. The transition is only deemed complete when all tasks have been completed and agreed between the Roc transition team, Roc Service teams and the customer.

A key aspect of the transition will be Roc performing a Due Diligence exercise on the existing IT environment. This will aid understanding but also ensure the IT infrastructure is in a healthy and comparable state to that outlined in the tender. As part of this exercise, Roc will provide the customer with a Red/Amber/Green (RAG) report on the state and health of their IT service.

To achieve the results and the return on investment for the customer, the transition needs to be successfully delivered on time and within budget. Roc places an emphasis on delivering effective project management of the transition process.

As a part of the transition, our standard PRINCE2 aligned, 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.

At project initiation, key milestones will be jointly agreed upon with the customer. For transitioning into Roc service, the following process is followed:

- **Discovery.** Gathering of relevant technical, service, and commercial information. This includes details on existing infrastructure, applications, services, and processes.

- **Operating Model.** Assessing and defining the service team to deliver the service specified.
- **Service Design** and Plan defined between both parties. Including agreement on Roles and Responsibilities for both the customer and Roc. The Service Design will ITIL processes, interaction and communications between all parties involved in the delivery of the Roc Managed Service.
- **Onboarding Plan.** Definition of an onboarding phase (typically 6 to 8 weeks) for Service Desk agents.
- **Secure connectivity** between the customer and Roc. Also, gather system credentials and store them in a secure vault.
- **Toolset Deployment.** Deployment of required ITSM and support toolsets.
- **Process and Procedure Definition.** Operating Procedures and Quick Reference Guides are written, updated, and agreed upon as necessary.
- **Knowledge Management and transfer.**
- **Service process testing, resiliency, and validation.**
- **Business Continuity and Disaster Recovery** updates within Roc, to ensure service availability.
- Project Support and Project Management activities
- Acceptance into Roc Service.

Following the start-up period, operational documentation and procedures are produced, tailored, and adapted for a seamless transfer into the Roc service desk. Any enhancements or optimisations can therefore be incorporated into the Service Design and conversely, any omissions or problems in the existing processes can be identified and rectified during the Discover Phase and be rolled into the Design, Build, and Manage phases.

Once developed, the operational and support documentation is agreed upon and signed off by the customer, stored in the centralised systems information database, and placed under change control.

Roc will only take customer systems into service once Roc service teams, the project team, and the customer have agreed the systems are fully documented and fit for purpose.

The illustration below outlines the key artefacts included in our service transition process:

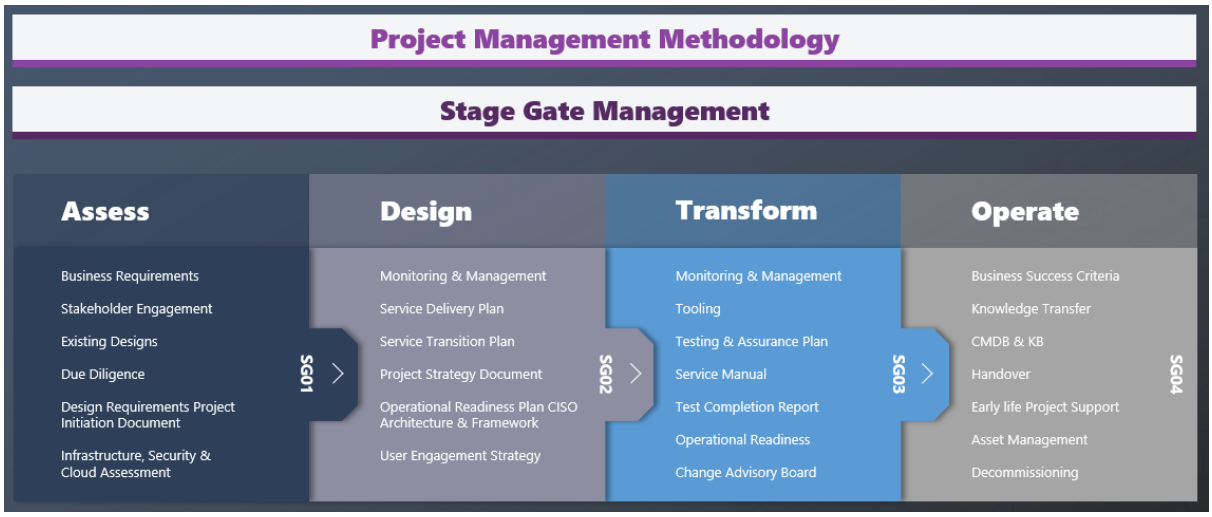

Figure 8 – Service Transition Methodology

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.