Managed Services

G Cloud 14

Roc

Contents

Document Information

CLIENT NAME	**G CLOUD 14**
PROJECT NAME	Managed Services
DOCUMENT AUTHOR(S)	Gill Brown

Document Change Record

ISSUE	DATE	DESCRIPTION
V0.1	24/04/24	First draft for sign off
V0.2	07/05/24	Final

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 publicsector@roctechnologies.com

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.

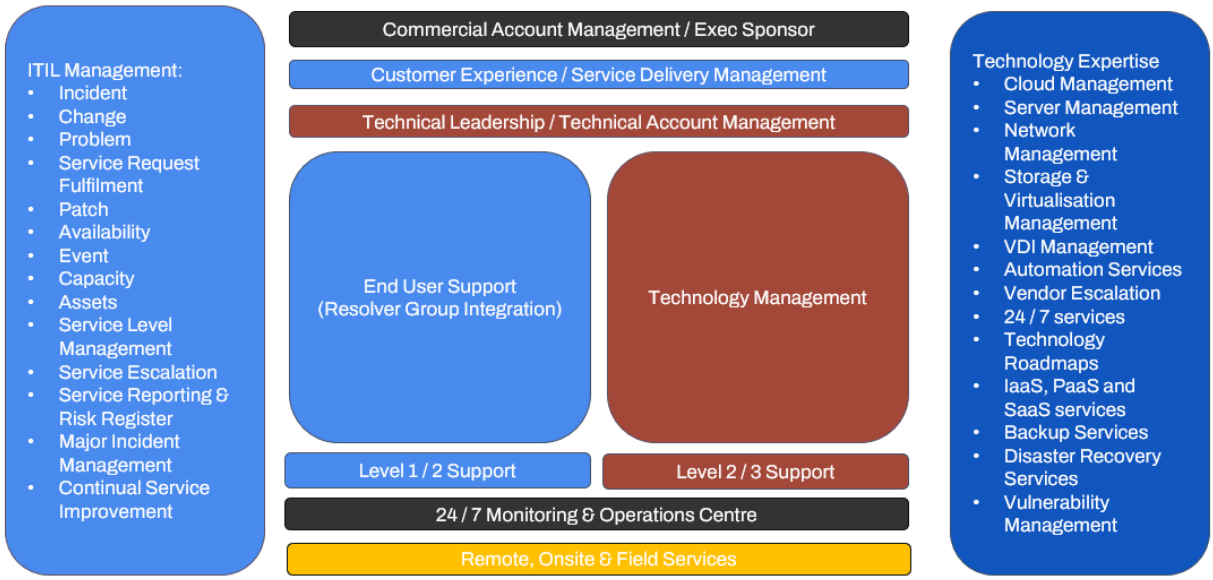

Figure 1 – Roc Managed Service Capability

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)
- 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 Technical Account Manager (TAM) can be included to provide technical leadership and authority for the Managed infrastructure.
- TAM to 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 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.
- An Infrastructure management service.
- 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.
- Technology management of Cloud platforms including Microsoft 365 and Azure, Amazon AWS, Juniper Mist, Zscaler and Aruba Central.

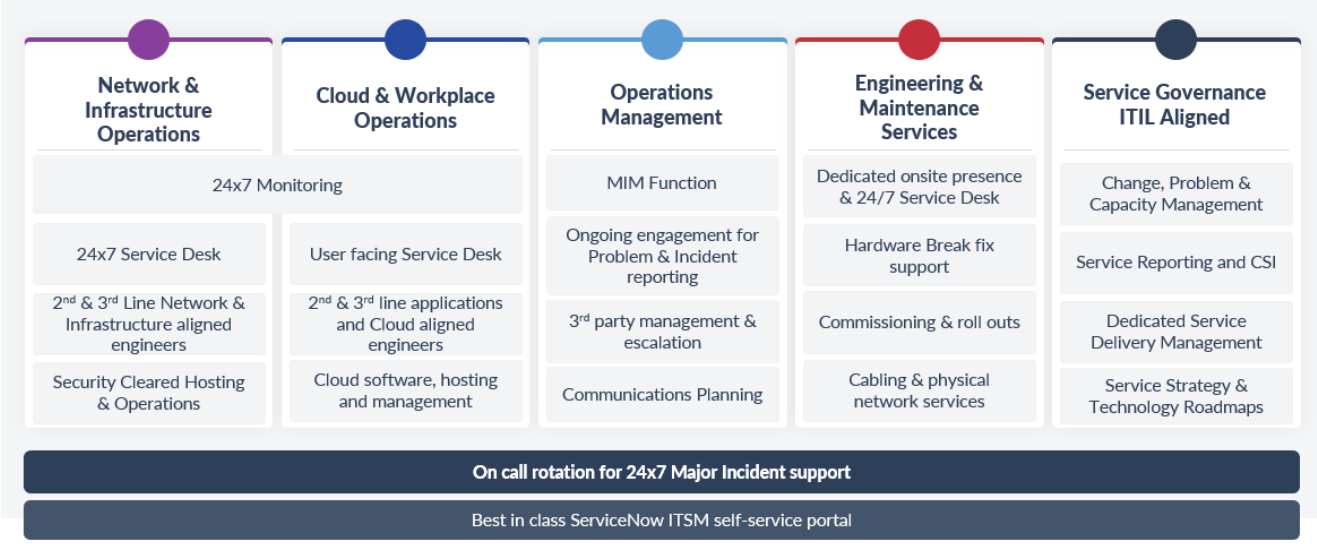

Figure 2 – Roc Operational Services

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

- **Contact Management.** Providing telephone, email, chat and portal functions via Roc's ITSM ServiceNow toolset and maintaining Technical Points of Contact (TPOC) for the service
- **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.
- **Event Management**. Roc operates a comprehensive managed service platform that includes monitoring and alerting for numerous aspects of an IT estate. Critical monitoring alerts are automatically reported directly to the Roc Service Desk on a 24x7x365 basis, 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.
- **24 x 7 Infrastructure monitoring.** The monitoring coverage will be on a 24x7x365 basis and will provide thresholds for critical system metrics with automatic alert generation in event of exceeding the thresholds. The alerting to be put in place will be determined during service take-on, but where applicable Roc will utilise its existing Kaseya monitoring.
- **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 have 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.

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

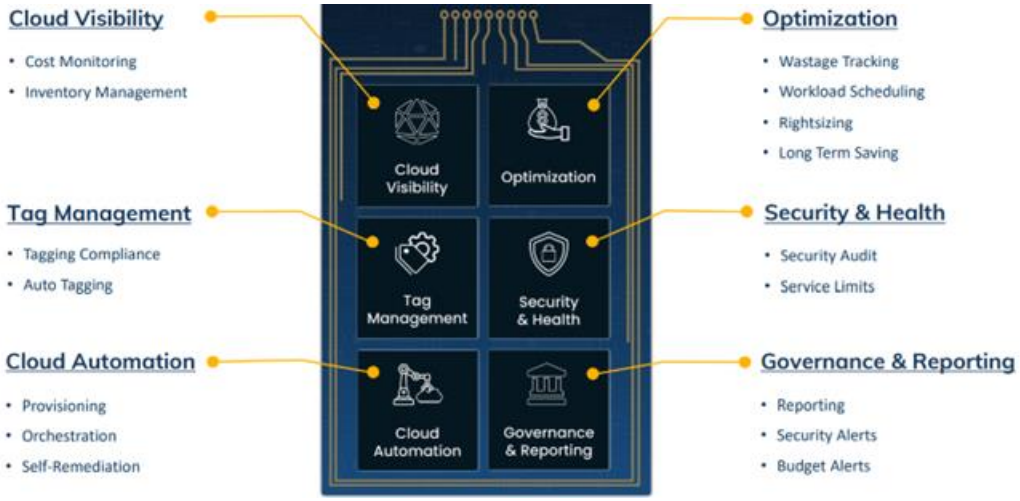

Figure 3 – Cloud Management Methodology

2.2 Support Model

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 and Cyber Essentials standards, as well as ISO 20000, ISO 27001, ISO 9001 and ISO 14001.

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

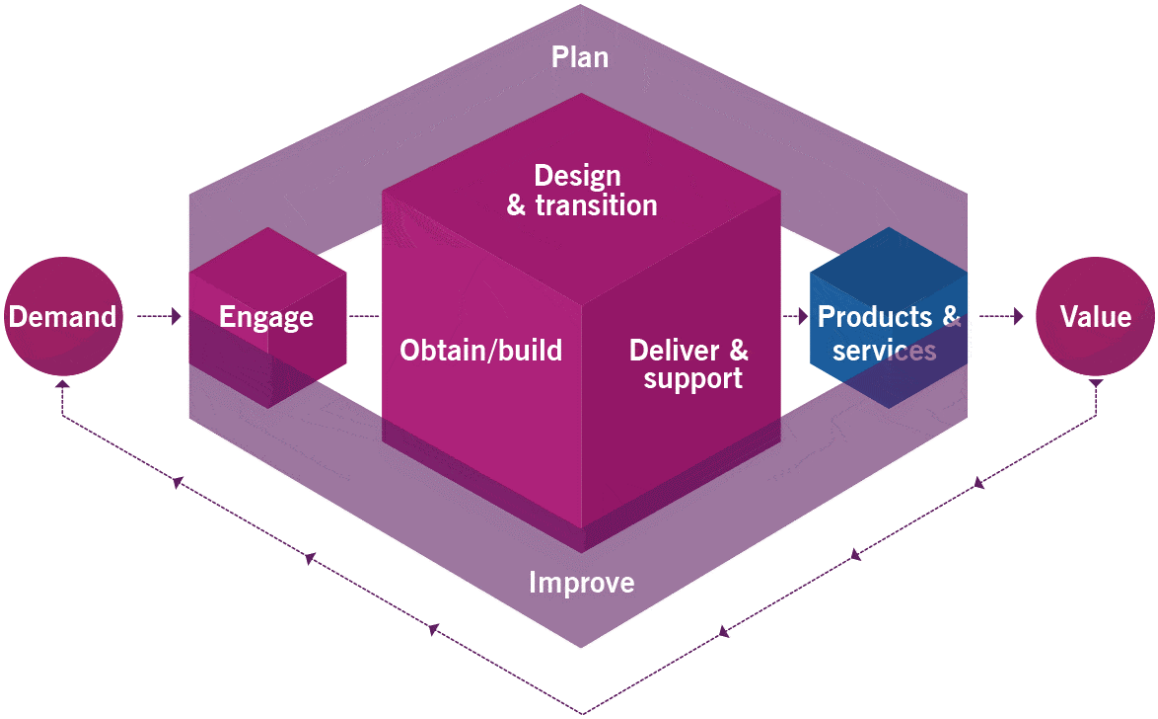

Figure 4 – ITIL Framework

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 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.

2.6 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.

2.7 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.

2.8 Service Level Agreements

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

2.8.1 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

2.8.2 Incident Management

PRIORITY	DEFINITION	TARGET RESPONSE	TARGET UPDATE	TARGET RESOLUTION
P1 (Critical)	Critical Business Impact. A complete service failure or severe degradation of service. Typically impacting >50% of users at a supported site, or >50% users of a supported system. No acceptable workaround available. Examples include: - • Complete network failure • Simultaneous failure of resilient WAN links • Core application/service down	30m	1h	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	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

2.8.3 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

2.8.4 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.

2.9 Service Delivery Management

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

PACKAGE	DESCRIPTION
Standard	• Standard Roc Service Report Template. • Quarterly service review performed remotely.
Enhanced	• Customised/Bespoke service report template • Monthly or quarterly service reviews performed remotely. • Quarterly onsite service reviews with aligned SDM. • Tailored observations & recommendations. • Continual Service Improvement Plan (CSIP).

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

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

2.10 Continuous Improvement

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

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

2.11 Service Pricing

Refer to Roc's pricing document.

2.12 On-boarding

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

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

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

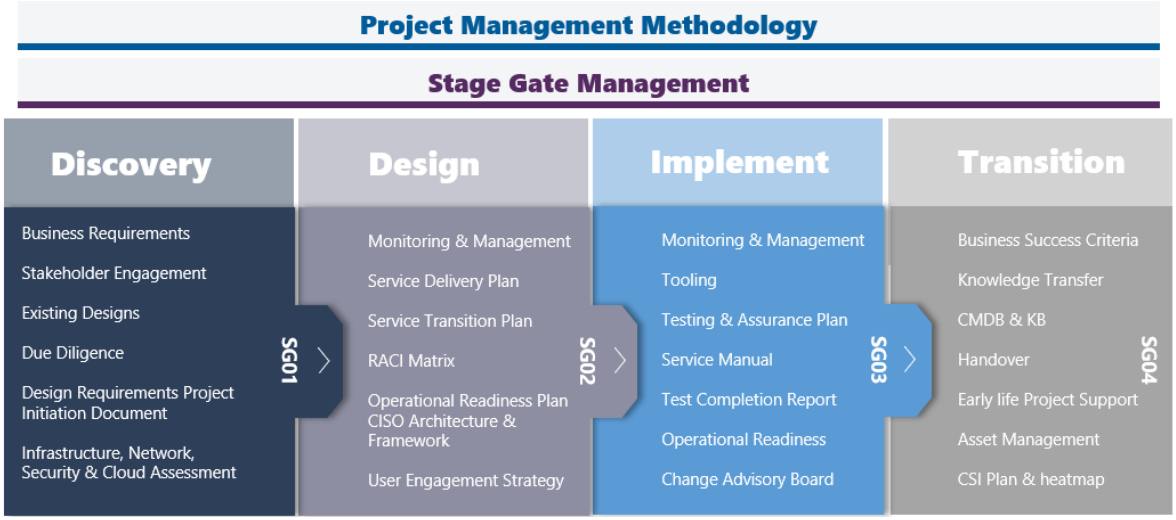

Figure 5 – Roc Service Transition Process

2.13 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.