Service Definition: SASE

Crown Commercial Services | G Cloud 15 framework

Contents

Document Information

Client name	G Cloud 15 Service Definition
Project name	SASE
Document author(s)	David Gearing, Gill Brown

Document Change Record

Issue	Date	Description
V0.1	01/12/25	Draft Template
V0.2	12/12/25	Draft Initial Content added
V0.3	22/01/26	Draft review and sign off
V1.0	27/01/26	Final for issue

Contact Information

This document has been supplied by Roc Technologies Limited, whose registered office is:	Roc Technologies Limited 1 Lindenmuth Way Greenham Business Park Greenham Thatcham RG19 6AD United Kingdom
Please refer all enquiries to:	**Gill Brown, 0845 647 6000** publicsector@roctechnologies.com.

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without the express written permission of Roc Technologies Limited and shall be held in safe custody.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

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. Whatever the requirement, Roc can manage all your hardware and software needs, from servers and desktops to applications, data, and networks. We support our customers throughout the IT lifecycle, from initial strategy development and technology assessment - through to innovative design and procurement processes, implementation, and management.

Secure Access Service Edge (SASE) is a core component of Roc's Platform business unit, bringing together networking and security into a unified, cloud-delivered service. Roc designs, implements, and manages highly secure, scalable SASE architectures for some of the UK's most demanding and security-conscious organisations.

Roc delivers a full range of SASE services, enabling secure connectivity for users, devices, applications, and data regardless of location. Our services support transformation across remote access, SD-WAN, cloud security, Zero Trust Network Access (ZTNA), and secure internet access for campus, branch, cloud, and home-office environments. We meet all scales of requirement, from targeted consultancy engagements to full SASE transformation programmes.

Roc has a highly skilled Project and Engineering team providing end-to-end delivery of SASE solutions. This includes architecture design, policy definition, identity integration, implementation, migration, consultancy, support, and fully managed SASE services.

Roc's SASE offering delivers cloud-native, globally distributed networking and security services using industry-leading vendors. Solutions may integrate with existing network infrastructure or form part of a broader network and security refresh supplied and provisioned by Roc.

Features and benefits of Roc's SASE offering include:

- Design, supply, and implementation of SASE and Zero Trust architectures.
- Converged networking and security services delivered from the cloud.
- Secure access for users, devices, and applications from any location.
- Unified management of SD-WAN, ZTNA, Secure Web Gateway (SWG), CASB, and Firewall-as-a-Service (FWaaS).
- Centralised policy definition and enforcement based on identity, device posture, and context.
- Zero Trust access controls replacing traditional VPN models.
- AI-driven threat detection, policy optimisation, and faster root-cause analysis.
- Consistent security policy enforcement across branch, cloud, and remote users.
- Inline traffic inspection and continuous risk assessment for users and applications.
- Comprehensive visibility, reporting, analytics, and compliance insights.

- Optimised application performance through intelligent traffic steering and cloud on-ramps.
- Secure enablement of cloud and SaaS applications.
- APIs and integrations to extend security operations and integrate with wider IT and SOC platforms.
- Proactive monitoring, incident response, and managed security operations.
- Accredited engineers delivering vendor-validated design, deployment, and operational best practice.

2. Service Description

Roc works with leading security and networking vendors to design, deploy, manage, and support Secure Access Service Edge (SASE) solutions. Roc's SASE offering delivers converged networking and security services from the cloud, enabling secure access to applications, data, and services for users and devices anywhere.

Roc's SASE offering includes the following service capabilities:

SASE Architecture Design, Scoping and Delivery:

- Requirements scoping and solution design for secure access and cloud-first networking.
- Design and delivery of SASE and Zero Trust architectures.
- Supply and provisioning of SASE components including SD-WAN, ZTNA, Secure Web Gateway (SWG), Firewall-as-a-Service (FWaaS), CASB, and DNS security.
- Cloud-native, globally distributed security platforms with optional on-premises or edge integrations.
- Roc works with leading SASE vendors to recommend best-fit solutions aligned to technical, security, and business requirements.
- Vendor-accredited engineers delivering best-practice, supportable, and compliant designs.
- Secure migration from legacy VPN, MPLS, and perimeter-based security architectures.
- Secure segmentation of users, applications, devices, contractors, and third-party access.
- Zero Trust access controls based on identity, device posture, and context.
- Professional Services to undertake deployment, migration, and policy configuration.

Management and Orchestration:

- Centralised, cloud-hosted management of networking and security policies.
- Unified policy definition across users, devices, applications, and locations.
- Zero-touch provisioning of edge devices and remote users.
- Identity-based access orchestration integrating with cloud and enterprise identity providers.
- Software-driven security enforcement across all access paths.
- Multi-tenant and role-based administrative access.

Security and Access Controls:

- Zero Trust Network Access (ZTNA) replacing traditional VPN connectivity.
- Least-privilege access enforcement to applications and services.
- Inline inspection of traffic for threats, malware, and policy violations.
- Secure Internet Access and SaaS protection through SWG and CASB capabilities.
- Continuous risk assessment and adaptive access policies.
- Support for secure access across branch, campus, cloud, and remote environments.

Analytics and Visibility:

- Centralised dashboards, reporting, and audit trails for security and compliance.
- End-to-end visibility of user activity, application usage, and access behaviour.
- Insight into security posture, risk levels, and policy effectiveness.
- Application performance and experience visibility across access paths.
- Actionable intelligence derived from security and access telemetry.

Automation and Programmability:

- API-driven SASE architecture for integration with IT and security platforms.
- Support for automation workflows using APIs, Webhooks, and orchestration tools.
- Automated policy enforcement and configuration consistency.
- Integration with SIEM, SOAR, ITSM, and SOC platforms.
- Auto-remediation and recommended actions based on policy and threat intelligence.

AI-Driven Security Operations:

- AI/ML-based threat detection and behavioural analytics.
- Enhanced identification of users, devices, and anomalous activity.
- AI-driven insights to pre-empt security incidents and misconfigurations.
- Automated incident correlation and prioritisation.
- Natural Language Processing (NLP)-based search, assistance, and troubleshooting.
- Integrated alerting, logging, and ticketing workflows.

User and Application Experience:

- Continuous monitoring of user experience and application performance.
- Visibility into latency, packet loss, and application response times.
- Optimised application routing and intelligent traffic steering.
- Secure enablement of SaaS, IaaS, and private applications.
- Root-cause analysis linking performance issues to access or security policies.

Identity and Device Context:

- Integration with enterprise identity providers and MFA platforms.
- Device posture assessment and compliance checks.
- Policy enforcement based on user role, device type, location, and risk.
- Secure onboarding for unmanaged, BYOD, and third-party devices.
- Support for hybrid identity and multi-cloud environments.

Monitoring and Reporting:

- Real-time monitoring of SASE service health and availability.
- Security event monitoring and access policy enforcement status.
- Configurable alerts, thresholds, and notifications.
- Standard and custom reporting for security, access, and compliance.
- Multiple export formats including PDF, CSV, and Email.

2.1 Product Portfolio

2.1.1 Cato Network

In today's hyper-connected and cloud-first world, organisations require security and connectivity that extends seamlessly beyond the traditional perimeter. Cato Networks SASE delivers a modern, cloud-native platform that converges networking and security into a single, globally distributed service, transforming how businesses securely connect users, locations, and applications.

With Cato's fully integrated SASE architecture, businesses benefit from a unified SD-WAN and security stack, delivering secure internet access, Zero Trust Network Access, firewall, and cloud security services from the edge. Built on a global private backbone and driven by continuous inspection and analytics, Cato simplifies operations, improves application performance, and enforces consistent security policies everywhere without the complexity of multiple point solutions.

With Cato Networks SASE, Roc enables organisations to deliver secure, high-performance access for employees, partners, and customers, wherever they work and however they connect.

2.1.2 Palo Alto Networks

In an increasingly distributed digital landscape, organisations need security and access that adapts to users, applications, and data wherever they reside. Palo Alto Networks SASE brings together best-in-class security and networking capabilities to create a unified, cloud-delivered platform designed for modern enterprises.

Powered by Prisma SASE and industry-leading threat intelligence, Palo Alto Networks delivers Zero Trust access, advanced threat prevention, and consistent security policy enforcement across users, branches, and cloud environments. With AI-driven security insights and continuous inspection, organisations gain deep visibility, simplified operations, and proactive protection against evolving threats all while enabling high-performance application access. With Palo Alto Networks SASE, Roc delivers a secure, scalable, and resilient access experience that empowers employees, customers, and partners to work safely and efficiently from anywhere.

2.2 Service Delivery

Roc offers packaged services for moving customers to a Cloud-managed network, using the approach below:

2.2.1 Support Model

The services within this document are designed to operate as a 2nd or 3rd line resolver group behind the client's principal end-user service desk. Where the client uses a separate desk, Roc expects that the clients service desk will employ reasonable efforts to 1) eliminate end-user error and 2) identify the most appropriate resolver group.

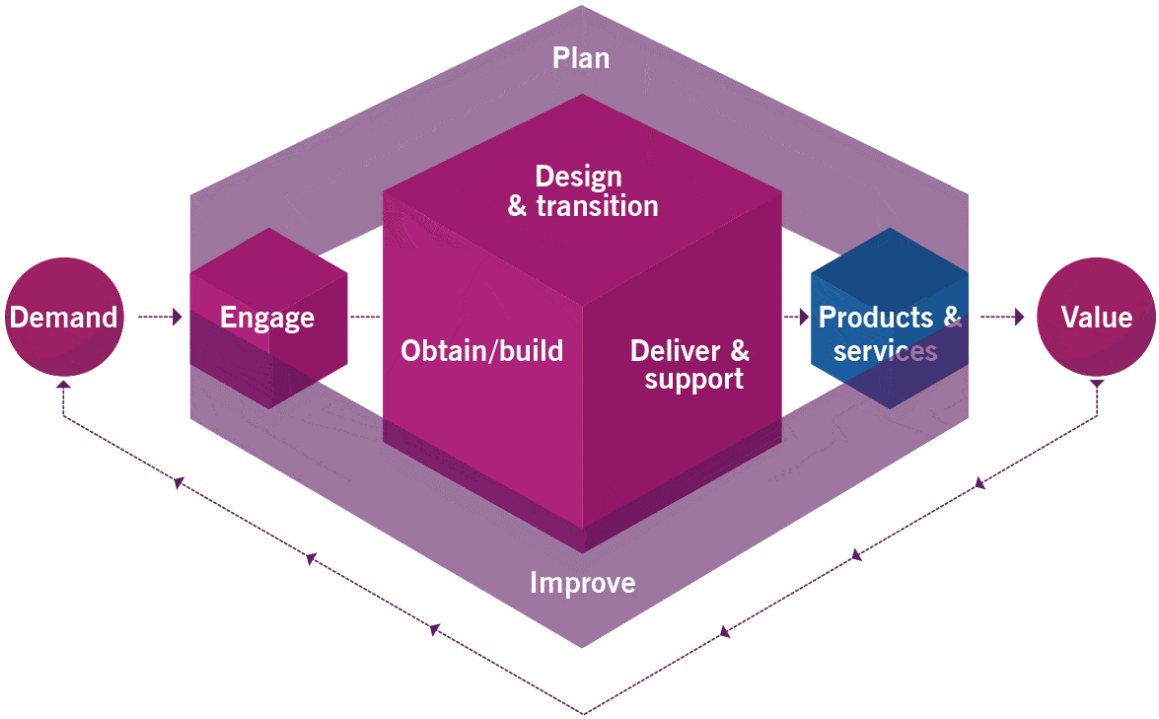
Additionally, where a separate 1st line desk is in use, Roc request that the clients service desk will operate during the same hours as the selected Roc service and manage communications amongst client stakeholders.

2.2.2 Accreditations & Vetting

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



2.2.3 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.

2.2.4 Support Agreements

To provide best value and consistent pricing, the services described within this document assume that existing customer software/provider/manufacturer support or warranty agreements will remain in-place and be accessible by Roc to facilitate a swift response to any security issues raised around third-party offerings.

2.2.5 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.

2.2.6 Change Management

It is assumed that each in-scope supported item will be fully managed by Roc, in line with the agreed change management process. Whilst the client and other 3rd parties chosen by them can retain administrative access (e.g. for emergency/auditing purposes), it is assumed that all changes to an in-scope supported item will be performed by Roc.

One hour of change management time per month is included for each in-scope supported item. This will be fulfilled during normal business hours. Additional service points can be purchased as required for the fulfilment of additional services.

2.3 Service Level Agreements

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

2.3.1 Hours of cover

Roc's Managed Services are offered based upon two standard hours of cover-

- Normal Business Hours: Monday to Friday, 08:00-18:00, excluding public holidays
- 24x7: 24 hours per day, 7 days per week, 365 days per year

2.3.2 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	15m	30m	4h
P2 (Serious)	Serious business impact. A widespread degradation of service, typically impacting all or a significant number (>25%) of users at a supported site, or of a supported system. Examples include: • Severe network performance degradation • Severe application performance degradation • Failure of non-resilient WAN links • Extended application functionality failure for all users • A loss of system resiliency	30m	1h	6h

P3 (Medium)	Medium business impact, A partial or intermittent degradation of service. Typically impacting a subset, group, or individual system users. Examples include: • Partial/intermittent network degradation • Partial/intermittent application degradation • System failure impacting individuals • Extended application functionality failure	2h	10h	16h
P4 (Low)	Low/minimal business impact. Typically, non-critical loss of service/functionality, or minor degradation of service for individual users. Examples include: • Network issues affecting lab/test Equipment • Applications issues when testing changes • Partial application degradation for individuals • Threshold breeches with no impact on service.	10h	20h	40h

2.3.3 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

2.3.4 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.

2.4 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.

2.5 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.

3. Service Pricing

Refer to Roc's pricing document representing service costs.

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.

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

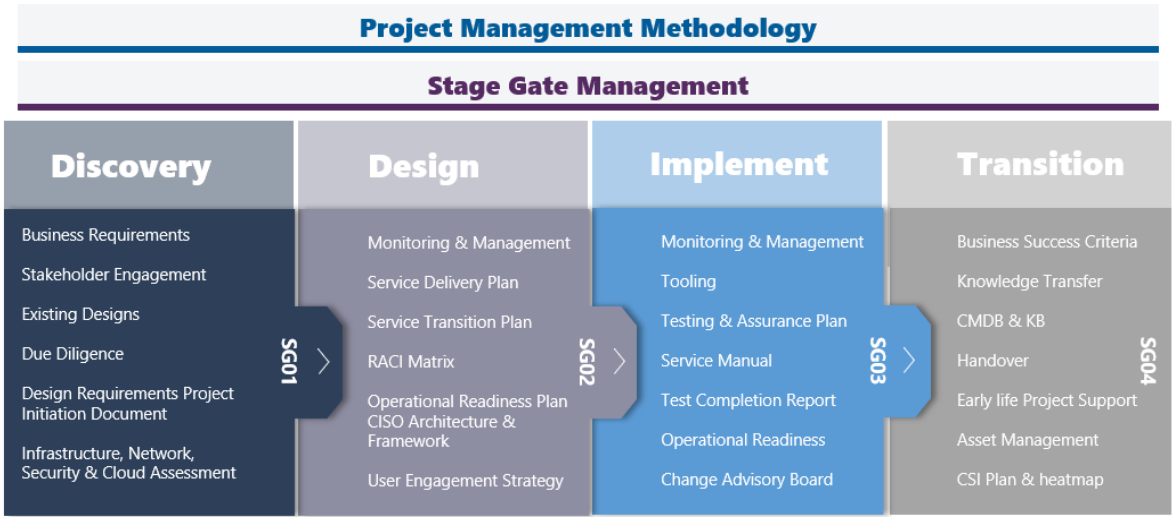


Figure 1 – Roc Service Transition Process

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.