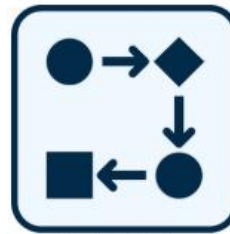


Proven to Deliver



Service Design
& Redesign



Cloud
Solutions



Project
Management



ICT
& Cabling



System
Training



Medical Records & Case
Management Systems



Business
Analysis



Service Desk
& Field Support

G-Cloud 15

Service Definition Document

SONAR CMS Analytics

1. Service Overview	Service Name	SONAR CMS Analytics
	Service Description	SONAR CMS provides secure, interoperable care management solutions that enable organisations to capture, share, and use information effectively across health and justice settings. The service supports continuity of care, data quality, reporting, and system integration to improve operational efficiency, clinical outcomes, and informed decision-making.
	Key Features	• Interoperability and system integration • Role based access control • Real time data visibility and reporting • Configurable windows • Cloud-hosted architecture • Data quality and validation controls • Audit trails and logging • Secure remote access • Standard-aligned information governance • Managed support and service delivery • Share information securely across systems without duplicate data entry • Access accurate records quickly to support timely operational decisions

		• Reduce manual administration through automated data flows and validation • Configure workflows to match local policies and service pathways • Track activity clearly to support audits and regulatory compliance • Manage user access safely using role-based permissions • Monitor performance in real time to identify and resolve issues early • Support remote working with secure, browser-based access • Improve data quality to increase confidence in reports and outcomes • Streamline service delivery through integrated support and reporting
2. Service Levels (SLA)	Support Levels	The SONAR CMS Cloud Support service is offered across four service level, Bronze, Silver, Gold, and Platinum, to align with differing operational/clinical requirements. All tiers provide access to 1st line Service Desk technicians, Field Engineer support, and 3rd line specialist support, with service hours increasing by tier, ranging from weekday business hours under Bronze, extended weekday and Saturday coverage under Silver and Gold, through to full 24/7 support under Platinum. Each level includes an allocated Service Delivery Manager, delivering structured service engagement via quarterly, bi-monthly, monthly, or weekly meetings with the Customer Clinical Director and key stakeholders, depending on tier. Specialist supplier support is provided on an annual allocation basis, ranging from 4-18 days per annum, supporting incidents, service requests, reporting requirements, and service optimisation activities, excluding development services. Training support is included

		across all tiers, delivered remotely via Microsoft Teams, to support new staff onboarding, process updates, and procedural changes, with allocations increasing by tier. Higher service levels also include dedicated Information Governance specialist support and programme management input to advise on IT requirements, future planning, and innovation. Gold and Platinum tiers further include proactive investigation of digital innovation opportunities within Health and Justice and the wider digital landscape.
	Support Channels	Email and phone support is available, seven days a week.
	Response and Resolution Time Targets	We used a tiered approach depending on your requirements. Response SLA are dependent on ticket priority.
	Availability	The SONAR CMS service is designed to be highly available and is supported by a structured Cloud Support service to ensure continuity of access and operational reliability. Availability covers both access to the SONAR service and the availability of support services, as defined in the contract. The SONAR service is delivered using resilient cloud hosting arrangements designed to support high availability, with continuous monitoring in place to identify and respond to service issues. The Cloud Support service provides guaranteed availability of the Service Desk, specialist support, and service management functions, aligned to the contracted Bronze, Silver, Gold, or

		Platinum service tier. Service Level Agreements (SLAs) define availability commitments, including target service availability, support coverage hours, and priority-based response and resolution targets. Service performance is monitored and reported through regular service reporting and reviewed during scheduled service management meetings.
	Resilience	The SONAR CMS service is designed to be resilient, with availability and continuity supported through a combination of robust cloud hosting arrangements and managed service controls. The service is hosted within resilient cloud datacentre environments that provide redundant infrastructure, high-availability architecture, and built-in fault tolerance to minimise the risk of service disruption. The underlying datacentre setup includes geographically resilient hosting, automated backup processes, and disaster recovery capabilities designed to support service continuity in the event of infrastructure or regional failure. Detailed datacentre architecture and location information can be provided on request where required. Service resilience is further supported by proactive monitoring, incident management processes, and defined escalation paths within the Cloud Support service. Regular service reviews are used to assess performance, identify risks, and implement preventative or corrective actions. Business continuity and disaster recovery arrangements are documented and tested to ensure the service can be restored within agreed timeframes. This

		layered approach ensures the SONAR CMS service remains reliable, secure, and resilient for users operating in critical health and justice environments.
4. Technical & Hosting	Technical Requirements	• Modern web browser supporting current security standards • Reliable internet connection for secure service access • Approved user devices meeting organisational security policies • User authentication managed through agreed identity controls • Role-based access configured for authorised users only • Secure network access allowing encrypted connections • Compliance with applicable information governance standards • Email access for service notifications and alerts • Customer-managed antivirus on end-user devices • Named technical contact for service coordination
	Hosting Locations	UK
	Scalability	The SONAR CMS service is delivered using segregated customer environments and controlled access to ensure one customer's usage does not impact another's service experience. Demand is managed through capacity planning, service monitoring, and prioritisation controls within the Cloud Support service. Support requests are handled independently per customer, with performance managed against agreed service levels. Regular service reviews are used to identify demand trends and implement

		preventative actions, ensuring consistent performance and service quality regardless of usage by other customers.
5. Constraints & Maintenance	Outage Reporting	The SONAR CMS service reports outages and service issues through structured communication and service management processes to ensure users are informed in a timely and transparent manner. Outages and service degradation are communicated to customers via email alerts to nominated contacts, providing details of the issue, impact, and progress updates until resolution. Email notifications are used for both planned maintenance and unplanned incidents. Service status information can also be made available through service reporting updates provided by the Service Delivery Manager. Where required, access to a service status dashboard can be provided to authorised users, presenting high-level information on service availability and incident status. Detailed technical status information is available on request. The service does not currently provide a public API for outage reporting. However, incident and outage information can be shared in structured formats as part of service reporting or through agreed integration methods if required.
	Service Constraints	SONAR CMS is a bespoke software that can be built upon depending on end user needs.
	Onboarding Process	Step-by-step process for new customer/user setup and initial data migration.

6. Onboarding & Offboarding	Getting Started	Users are supported to start using the SONAR CMS service through a structured onboarding and enablement approach delivered as part of the Cloud Support service. Onboarding begins with an initial discovery session to confirm service scope, user roles, access requirements, and integration dependencies. Users are provided with online training sessions, delivered remotely via Microsoft Teams, covering core system usage, operational workflows, and support processes. Training is tailored to user roles and includes opportunities for questions and guided walkthroughs. Where required, onsite training can also be provided, subject to agreement, to support organisations that benefit from face-to-face delivery. Comprehensive user and support documentation is supplied in accessible digital formats, including onboarding guides, process documentation, and quick-reference materials, enabling users to learn at their own pace and refer back as needed. An allocated Service Delivery Manager coordinates onboarding activities and acts as a point of contact throughout the early stages of service adoption. Ongoing assistance is provided via the Service Desk, ensuring users receive timely support as they begin using the service and embed SONAR CMS into day-to-day operations.
---	-------------------------------	---

	End-of-contract data extraction	When a contract for the SONAR CMS service ends, users are supported to extract their data in a structured and secure manner as part of the offboarding process. Data extraction requirements are confirmed during offboarding planning to ensure alignment with the customer's operational and information governance needs. Data can be provided in commonly used, open formats, such as CSV or other agreed structured formats, to support reuse or migration to alternative systems. The scope of data extraction includes customer-owned operational and reporting data held within SONAR CMS, excluding supplier proprietary materials. Extraction is coordinated by the Cloud Support team, with oversight from the Service Delivery Manager, and delivered using secure transfer methods agreed with the customer. Clear timelines are agreed in advance to minimise disruption and ensure continuity of service. Users retain full ownership of their data throughout the contract. Any temporary access required to support data extraction is managed using role-based access controls. Following confirmation of successful data transfer, access to the service is withdrawn in line with agreed offboarding procedures and data retention policies

7. Security	Governance	The SONAR CMS service operates under a formal information security management framework aligned to ISO/IEC 27001 principles and UK public sector information governance requirements. Information security policies cover areas including access control, data protection, incident management, risk management, change control, supplier management, and business continuity. Responsibility for information security sits with a designated senior information security lead, supported by operational security and service management teams. Security responsibilities and escalation routes are clearly defined, ensuring issues are reported, assessed, and addressed promptly. Policies are communicated to staff through mandatory onboarding and refresher training, supported by documented procedures and guidance. Compliance is enforced through role-based access controls, segregation of duties, and formal approval processes. Adherence to policies is monitored through regular reviews, audits, and service reporting. Information security incidents are managed through a defined incident response process, including investigation, containment, and customer notification where required. Policies and processes are reviewed regularly to reflect changes in risk, regulation, or service delivery, ensuring continued compliance and effective protection of customer data.
	Vulnerability Management	Vulnerability management for the SONAR CMS service follows a defined internal process. Potential threats are assessed using risk-based

		evaluation, considering severity, exploitability, and impact on service availability and data security. Information about threats is gathered from supplier security advisories, vendor notifications, vulnerability bulletins, and internal reviews. Identified vulnerabilities are logged, prioritised, and tracked through to resolution. Critical and high-risk patches are deployed as soon as practicable, following testing and approval through change management processes, while lower-risk updates are scheduled as part of routine maintenance. This ensures timely remediation while maintaining service stability.
	Protective monitoring approach	Protective monitoring for the SONAR CMS service is delivered through defined internal monitoring and alerting processes. Potential compromises are identified using system logging, access monitoring, service alerts, and operational reviews to detect unusual or unauthorised activity. When a potential compromise is identified, it is logged, investigated, and escalated in line with the incident management process. Security incidents are prioritised based on risk and impact, with high-risk incidents responded to immediately and managed through defined escalation routes. Customers are notified where required, and corrective actions are implemented promptly to reduce risk and prevent recurrence.
	Access Restrictions	Access to SONAR CMS management interfaces and support channels is restricted using role-based access control (RBAC). Access is granted only to authorised users based on their role and responsibilities, following approval by nominated customer or supplier administrators. Permissions are limited

		to the minimum required to perform assigned tasks, supporting the principle of least privilege. Management interfaces are protected by secure authentication controls, and access is reviewed regularly. Support channel access is similarly controlled, ensuring only approved users can raise or manage service requests, reducing the risk of unauthorised access or data exposure.
	Account Management	Allocated Service Delivery Manager, delivering structured service engagement via quarterly, bi-monthly, monthly, or weekly meetings with the Customer Clinical Director and key stakeholders, depending on tier.
8. After Sales Support	Change Management	Configuration and change management for the SONAR CMS service follows a formal, documented process aligned to IT service management best practice. Service components and configurations are recorded and tracked throughout their lifecycle, including initial setup, changes, and decommissioning. All change requests are logged, assessed, and approved prior to implementation. Changes are evaluated for operational and security impact, including access control, data protection, and compliance considerations. Higher-risk changes are subject to additional review and testing before deployment. This approach ensures controlled change, traceability, and continued service security.