SAYARI

Map Service Definitions

G-Cloud 15 Sayari Ltd.

Sayari Map

Service Definition

Table of contents

1 Introduction 4
1.1 Document structure 4
1.2 How to use this document 4
2 Service description 5
2.1 About our service 5
2.2 Delivery framework 5
2.3 Service features and benefits 6
2.4 Service scope 6
2.4.1 Service constraints 6
2.4.2 System requirements 7
2.5 User support 7
2.5.1 Support details 7
2.5.2 Accessibility and usability 7
2.6 How users work with our service 8
2.6.1 Browsers 8
2.6.2 Desktop application 8
2.6.3 Service interface 8
2.6.5 API 8
2.6.6 Accessibility and usability 8
2.6.7 Customisation 9
2.6.8 Service levels and availability 9
3 G-Cloud alignment information 10
3.1 Section introduction 10
3.2 Onboarding and offboarding processes 10
3.2.1 Onboarding 10
3.2.2 Offboarding 10
3.3 Data 10
3.3.1 Data importing and exporting 10
3.3.2 Analytics 11
3.3.3 Independence of resource 11
3.3.4 Public sector networks 11
3.3.5 Data-in-transit protection 11
3.3.6 Asset protection 11
3.4 Availability and resilience 12
3.4.1 Guaranteed availability 12
3.5 Governance 12

3.6 Security 12
3.6.1 Operational security 12
3.6.2 Staff security 13
3.6.3 Secure development 13
3.6.4 Identity and authentication 13
3.7 Auditing 13
3.7.1 Performance monitoring and metrics 13
3.7.2 Compliance and quality management 14
3.8 Backup, restore & disaster recovery 14
3.9 Training 14
3.10 Service pricing 15
3.11 Invoicing process 15
3.12 Termination terms 15
4 Security and data governance 16
4.1 Data protection and encryption 16
4.2 Data at rest, storage locations, and physical security 16
4.3 Data sanitisation and disposal 16
4.4 Security testing and assurance 16
4.5 Incident and protective monitoring management 16
4.6 Configuration and change management 16
4.7 Information security management and certifications 17
4.8 Secure development and cryptography 17
4.9 Identity and access management 17
5 Supplier information 18
5.1 About us 18
5.2 Relevant experience and testimonials 18
5.3 How to buy 18

1 Introduction

1.1 Document structure

Supporting you to understand the scope, functionality, security, pricing and management of our services, this document outlines the services provided by Sayari Map under the G-Cloud 15 Framework. This document is organised into 3 clear sections:

- **Service description:** An overview of our services, detailing key features, benefits, delivery approach and assurance measures
- **Operational delivery and framework alignment:** Explaining how our services are delivered in line with the requirements and standards of the G-Cloud 15 framework
- **Supplier information:** Provides a summary of our organisation, mission, relevant experience and instructions on procuring our services via G-Cloud

1.2 How to use this document

From initial service evaluation through to contract award and ongoing delivery management, this document is designed to support buyers throughout every stage of their G-Cloud procurement process, including:

- **Early stage evaluation:** Section 2 (Service description) outlines our service scope, delivery methodology and key benefits to help buyers assess alignment with organisational needs
- **Due diligence and contract preparation:** Section 3 (G-Cloud alignment information) provides guidance on onboarding, service levels, data management, support arrangements and exit procedures
- **Data protection and compliance assurance:** Section 4 (Security and data governance) explains our information security framework, data handling standards and business continuity measures
- **Supplier verification:** Section 5 (Supplier information) presents background information about Sayari, alongside relevant accreditations and available procurement routes

2 Service description

2.1 About our service

Drawing on **10 years** of experience, we are a risk intelligence provider that equips intelligence professionals with immediate visibility into complex commercial ownership and control, and trade relationships.

Sayari Map is a supply chain mapping and risk intelligence platform. Providing complete visibility of the supply chain, Sayari Map uses international corporate data and supply chain records to allow risk identification and monitoring and adjudication workflows.

To support our clients in exposing hidden risk across their corporate and trade networks, Sayari Map allows you to dive into the different entities throughout your supply chain. To improve visibility of your supply chain and allow you to drill down on specific suppliers, you can undertake product-specific supply chain mapping.

Sayari Map can be used in conjunction with other Sayari products, including Sayari Graph. Graph is a commercial risk intelligence platform that combines global corporate and supply chain data, complex entity networks, and intuitive risk identification to accelerate investigative, intelligence, and due diligence activities.

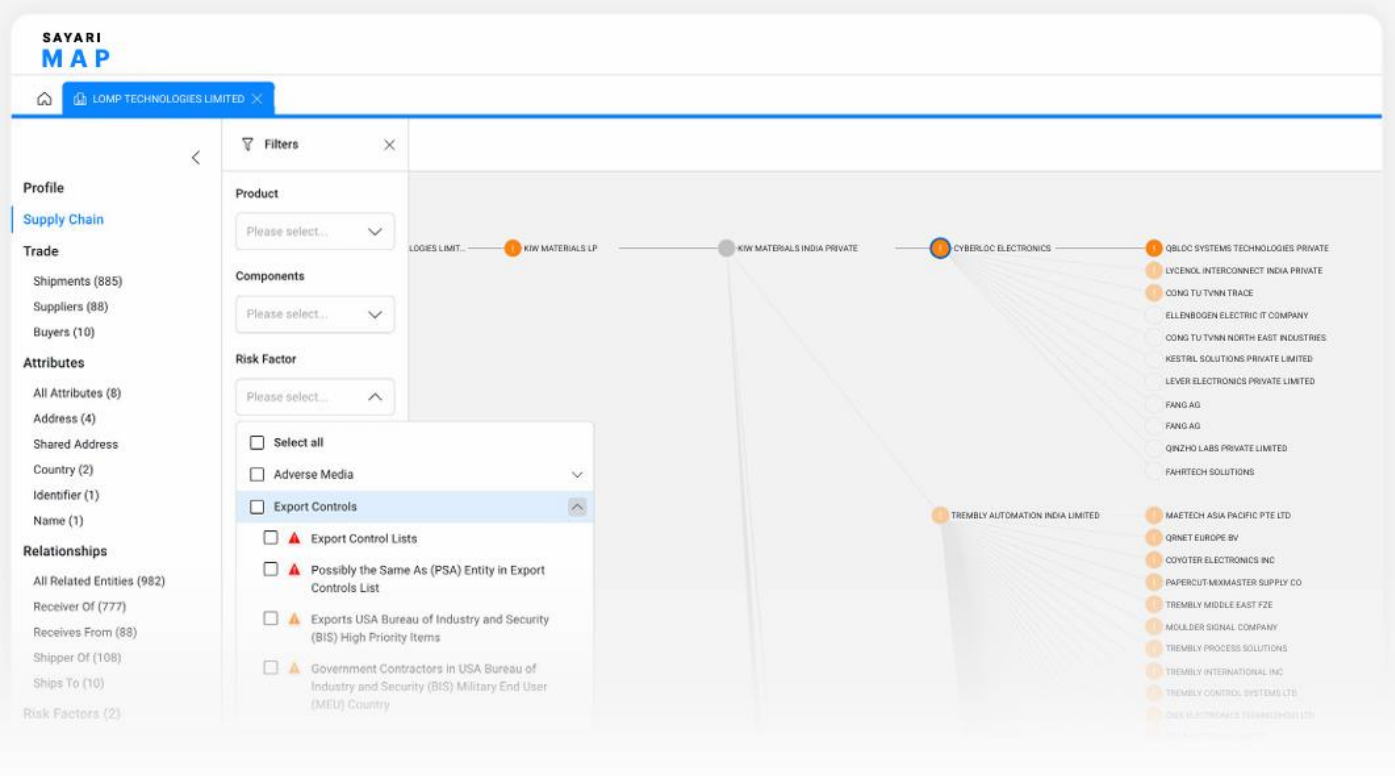


Figure 2.1: Sayari Map

2.2 Delivery framework

Ensuring our software meets customer requirements, we follow a standard Software Development Lifecycle (SDLC) framework. Incorporating industry best practices across the full lifecycle, we complete:

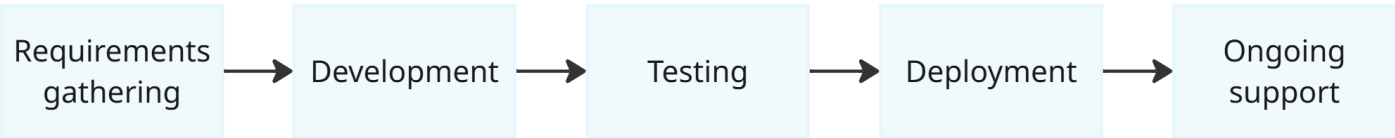


Figure 2.2.1: Our SDLC framework

We follow a structured SDLC approach for all projects, with documentation covering change management, quality assurance and approval procedures. Equipping our staff to deliver successful and repeatable transformations, all our staff are trained in SDLC.

2.3 Service features and benefits



Product-specific supply chain mapping: Sayari Map allows our clients to quickly identify product-specific supply chains from raw material to the end client. By being able to isolate potential risk to specific products, our clients can identify which business units and relationships leave them open to exposure.



Instant risk identification and classification: Our system efficiently prioritises explicit and potential threats with Sayari Risk Factors. Sayari provides access to more than 500 risk factors across 6 thematic categories, including sanctions, forced labour, export controls, political exposure, regulatory action, and adverse media. These risk factors enable users to quickly and confidently assess an entity's risk exposure and gain instant visibility into precise risk landscapes across complex, cross-border business and trade relationships.



Comprehensive, global data: We leverage the broadest corporate risk intelligence dataset available. This consists of over 10 billion records on over 850 million corporations and 800 million key individuals from over 250 jurisdictions around the world. Sayari Map covers high-risk and hard-to-source geographies like China, Russia, Iran, Venezuela, Mexico and Turkey.



Seamless integration and deployment: We allow our clients to get started with the enterprise-ready platform your investigative and analytical teams need. It has flexible deployment, easy integration, and the peace of mind that your data and insights are never shared. Adapting to diverse customer use cases, Sayari Map allows for customisable scoring and workflow configurations.



Automated, instant mapping: Increasing efficiency for users, Sayari Map provides near-instant, up-to-date visibility into supplier networks. To achieve this, Sayari Map completes automated upstream mapping. Allowing users to focus on actionable insights and avoid being overwhelmed by false positives, product blueprints reduce irrelevant risk alerts by 57%.



Evidence-based, transparent risk factors: Allowing users to quickly understand and communicate risks, Sayari Map's risk factors are fully evidence-based and traceable to source data. Ensuring stability, reliability and instant availability without reliance on third-party providers, Sayari offers direct, in-house access to premium data.

2.4 Service scope

Providing flexibility for clients, Sayari Map has the following deployment options and configuration characteristics:

- **Service Type:** Cloud-based application
- **Add-on or Extension:** No
- **Cloud Deployment Model:** Sayari Map is available as a multi-tenant cloud application

2.4.1 Service constraints

Sayari Map exclusively provides solutions for defence and national security, law enforcement, central government departments, critical national infrastructure, and healthcare. The constraints on our system are limited to:

Maintenance windows

Sayari application and data releases do not require maintenance windows, allowing our clients have access to the most recent data available without access to the system being impacted.

In the unlikely event a window is required, it will be scheduled between 9:00 pm Friday and 1:00 am Monday Eastern Time, not to exceed a total of 4 hours in one month. To provide visibility, maintenance windows are communicated to clients ahead of the scheduled time. This is communicated by email and followed up by the Customer Support Manager (CSM).

Licenses

Licenses must be assigned to individual, named users, each with a dedicated and unique email address. All licenses will be provisioned on a single-user basis. For secure or restricted customers, we have a governed process in place to obfuscate email credentials while maintaining compliance with licensing requirements.

2.4.2 System requirements

Sayari Map is a cloud-based application which can be accessed worldwide once the user's identity has been confirmed through username and password. To access the Sayari Map application, our clients only require an internet browser (with a 2014 release date or later).

The Global Data File and REST API technical requirements vary based on client infrastructure, as discussed during onboarding with each client.

2.5 User support

To ensure our buyers can access help, resolve issues efficiently and maintain continuity of operations, we provide our buyers with access to **24/7 support.**

2.5.1 Support details

Ensuring that our clients always have access to support is paramount to Sayari. Managed by the buyers' dedicated Customer Success Manager (CSM), Sayari provides an in-tool feedback function. The CSM will support customers from 9 am to 5 pm Monday to Friday. The CSM will act as the main point of contact and aim to acknowledge all queries on the same business day.

Providing a point of escalation, where an issue cannot be resolved by your dedicated CSM, the CSM will escalate the issue to our Senior Management Team (SMT). Securing the necessary oversight, our SMT will deploy the necessary resources to achieve a solution.

Sayari Global teams provide service management support for platform incidents outside of UK business hours.

2.5.2 Accessibility and usability

Sayari Map is designed to be accessible to all users. To achieve this, we:

- Ensure all interfaces and documentation comply with WCAG 2.1 AA standards
- Perform accessibility testing during every major release, in line with Section 508
- Provide documentation in HTML and PDF formats that meet accessibility guidelines, with buyers able to request alternative formats if required
- We continually review accessibility feedback through our user-centred design process and customer feedback loops. Improving our solutions, we integrate improvements into subsequent releases

2.6 How users work with our service

2.6.1 Browsers

For our SaaS application, our clients only require a standard internet browser with a 2014 release date or later. Supported browsers include:

- Internet Explorer 11
- Microsoft Edge
- Firefox
- Chrome
- Safari
- Opera

We recommend enabling JavaScript and cookies for full functionality. Buyers are notified in advance of any changes to browser support.

2.6.2 Desktop application

A dedicated desktop application is not required.

2.6.3 Service interface

Sayari's Map product provides automated, evidence-based supply chain mapping and risk identification, enabling organisations to instantly visualise their complete supply chain networks and identify hidden compliance risks. This product goes beyond traditional questionnaire-based approaches by leveraging real trade transactions and authoritative data sources to deliver transparent, verifiable supply chain intelligence for navigating UFLPA, ICTS, and other fast-evolving regulations.

For organisations seeking immediate supply chain visibility without relying on time-consuming surveys, Sayari Map delivers evidence-based mapping using real trade data, empowering you to instantly identify multi-tier risks and ensure regulatory compliance with complete source documentation.

Sayari Map is a web application streamlining high-volume supplier screening, enabling users to automatically and instantly map product-specific upstream supply chains and identify sub-tier suppliers and their associated risk. Sayari Map enables buyers to:

- Efficiently identify and manage supply chain risk
- Perform instant batch screening of n-tier supplier risk
- Create automated, product-specific supply chain mapping
- Conduct monitoring and adjudication workflows

2.6.5 API

API availability and documentation

- **API availability:** We provide a private API, Sayari REST. Product access is provided via API Credits that are consumed on a per-call basis
- **API capabilities:** Sayari REST API allows users to:
  - Run customised data enrichment services to process client and counterparty information
  - Validate and match submitted data against Sayari reference data
  - Enrich records with additional identifiers, including owners, directors, officers and upstream ownership information
- **Documentation:** Available formats include html found here: https://documentation.sayari.com/home/overview

2.6.6 Accessibility and usability

Ensuring all users can interact efficiently and effectively with Sayari Map, it is designed with usability as a core focus. Supporting users with diverse needs, Sayari Map meets recognised accessibility standards including

WCAG 2.2 AA and EN 301 549. Enhancing user experience, key features include keyboard navigation, screen-reader compatibility, high-contrast modes and scalable text.

2.6.7 Customisation

Our software has been designed to be user-friendly and easy to navigate. As such, we offer a limited ability to deliver customisation to the software. Supporting individual user needs depending on the project and investigation, we enable users to:

- Name their projects, folders, saved entities, records, search results and graphs
- Organise entities into projects and folders
- Upload their own data and match it against our data
- Input, add or modify information, with changes only visible within their organisation
- Upload a CSV file with up to 25,000 entities to check for coverage and receive direct links to entity profiles

Shaping our product strategy, we host regular customer events that facilitate direct engagement with our Product Managers to help inform product updates.

2.6.8 Service levels and availability

The following Service Level Agreements (SLAs) define the availability, responsiveness, and performance standards that apply to the service under the G-Cloud 15 framework.

Incident type	Communicated to the client within	Required resolution time
Major incidents	Within 12 hours	No more than 24 hours
Minor incidents	Within 12 hours	No more than 72 hours
Scheduled downtime	Within 12 hours of the event	N/A – although it will be planned around business hours

Figure 2.6.8.1: Our SLAs

These metrics are monitored continuously, with results reviewed monthly as part of service management reporting. Any breaches of SLA targets trigger internal escalation and, where applicable, corrective actions or service credits in line with the contract.

3 G-Cloud alignment information

3.1 Section introduction

Undertaking a collaborative approach, this section outlines how we work with client teams at each stage of delivery, from onboarding to training, live operation, support and secure offboarding. Adding value to our buyers and ensuring we adapt to the specific objectives, scale and governance requirements of each client, we:

- Provide our clients with access to Connect, our dedicated portal and customer hub, delivering dedicated, personalised support
- Allocate a dedicated CSM to each client, offering additional training and support
- Hold regular customer events that facilitate direct engagement with our Product Managers and help inform product strategy

3.2 Onboarding and offboarding processes

3.2.1 Onboarding

To provide support for clients, we offer individual user onboarding which includes solution roll out, initial training on the software and access to additional scheduled workshops. Typically, these onboarding sessions are completed within a week of the client signing the contract and are conducted remotely via Webex or other VTC program but may be delivered on-site when requested.

As part of the solution roll out, our clients receive sandbox testing accounts, technical configuration, and integration support to include mapping of data schemas and advising on entity resolution frameworks.

After sales support

For client service excellence, each of the Sayari products includes after sales support to all clients. Whilst this varies depending on product or level of product purchased, as a minimum it includes:

- Provision of a dedicated CSM as single point of contact who will ensure that each client is harnessing the software to achieve their aims. The CSM is available via email and phone during business hours and a special emergency line is provided outside of business hours for critical client needs
- A comprehensive training programme to support our clients in getting the best of the programme
- Access to Connect, providing a single customised collaborative workspace with targeted assets and resources
- Analytical support provided by Sayari's team of subject-matter experts
- Access to additional training sessions and workshops. This has included advanced product functionality, emerging typologies, and live case support integrating Sayari data and analytics

3.2.2 Offboarding

As an annual subscription model, at the end of the project or contract term, all users can download all saved work and any customisations.

To provide support to our clients, this data export function can be completed in a range of formats to ensure alignment to client needs. This includes CSV, XLS, PDF, JSON, and Parquet. Sayari Technical Teams can assist in removing bulk file data depending on the terms of our agreement.

3.3 Data

3.3.1 Data importing and exporting

Buyers can upload data using CSV formats.

As an annual subscription model, at the end of a project or contract term, all UI users can download all saved work and any customisations. Aligning with client needs, this data export function can be completed in a range of formats. This includes CSV, XLS, PDF and image files. To provide support to our clients, our Technical Team can assist in removing bulk file data depending on the terms of our agreement.

3.3.2 Analytics

Sayari provides standard service metrics, including:

- Daily logins
- Data consumption
- Utilisation of product features

To aid buyers in understanding if they are fully utilising our product, we report on the above metrics quarterly to our clients and their CSM. Adding value, this allows us to identify opportunities to provide additional training to our clients.

3.3.3 Independence of resource

Sayari has a standard SLA with monthly uptime and performance guarantees of **99%**. This is despite continuous growth in the number of users who access our system. To ensure that this remains the case and there is no impact to service, we regularly review our systems, service and personnel to guarantee capacity for all users.

3.3.4 Public sector networks

Sayari Map does not connect to public sector networks.

3.3.5 Data-in-transit protection

To ensure the confidentiality of data, we apply robust encryption protocols to protect all sensitive data, both at rest and in transit, using TLS 1.2+ encryption and data at rest using AES-256. As a Cyber Essentials+ certified organisation, we follow best practices aligned with ISO 27001 and National Cyber Security Centre guidance.

3.3.6 Asset protection

Customer data is stored within secure UK data centres that comply with recognised security standards, including:

- CSA CCM V3.0
- SSAE-16/ISAE 3401

These data centres provide robust physical access controls, such as monitored entry points, controlled access zones and continuous oversight.

Data sanitisation follows industry best practice, using cryptographic erasure or secure deletion techniques to ensure information cannot be recovered. Complying with recognised standards, including CSA CCM v.3.0, CAS (sanitisation) and ISO 27001, any end-of-life equipment is disposed of in line with our Data Destruction Policy. This includes secure wiping and physical destruction of all media before disposal.

3.4 Availability and resilience

3.4.1 Guaranteed availability

- Sayari maintains a **99%** monthly uptime Service Level Agreement with all Clients
- To reduce the impact to the service in the unlikely event of a critical outage, we backup data daily. Data restoration can be achieved within 24 hours to limit the downtime and subsequent impact on our clients
- The service is hosted across multiple UK data centres to ensure resilience and prevent downtime
- Our Recovery Time Objective (RTO) for a highly unlikely critical outage where all customer data is deleted is 48 hours
- Sayari's Recovery Point Objective (RPO) is within 1 second

3.5 Governance

Our services are delivered under a fully integrated management system. With over 2 billion business and personal records saved within Sayari Map, the security of systems and the data they hold is paramount. We operate in line with GDPR principles and are certified to ISO 27001, Cyber Essentials+ and SOC2 Type II.

To identify improvement opportunities and track corrective actions, our Security Engineering Division reviews performance data, customer feedback and audit findings monthly. Providing oversight, governance of all management systems is overseen by our VP of Information Security.

3.6 Security

We operate a suite of security and governance policies that detail the security processes that we follow. To ensure we remain aligned with industry requirements and our ISO 27001 accreditation, our policies are reviewed annually. Working in line with our policies, all staff receive training on these policies from our Security Engineering Division during their induction. Maintaining compliance, our Security Engineering Division completes annual audits across our business, documenting outcomes and implementing continuous improvement measures.

3.6.1 Operational security

Configuration and change management

Making sure our infrastructure is developed, deployed and maintained securely, we maintain a robust configuration and change management framework. Providing full accountability, version control and controlled change processes, source control and development workflows are managed through GitHub Enterprise.

Vulnerability management

To identify emerging threats, vulnerable systems and potential weaknesses in our processes, we leverage a range of open and closed source threat intelligence and conduct annual internal risk assessments. Patch management is driven by our Vulnerability Management Policy, with prioritisation determined by the severity and security implications of each vulnerability. Protecting our systems against current and evolving threats, security patches classified as critical or high impact are escalated and applied as quickly as possible to minimise exposure.

Protective management

To identify malicious activity occurring on our systems, we have implemented a centralised logging system. Providing oversight, our Security Engineering Team are responsible for maintaining our logging system and implementing our incident response process. This includes:

1. Detection
2. Analysis
3. Containment
4. Eradication
5. Recovery
6. Post-incident activity

Providing a rapid response for critical priority incidents, our Security Engineering Team will review and resolve any incidents within a 6-hour recovery window.

3.6.2 Staff security

All staff with access to systems or customer data undergo background screening that meets BS7858:2019 standards. Access is granted on a strict least-privilege basis and protected through Multi Factor Authorisation (MFA) and activity logging. Where required, our staff have additional government security clearance, up to and including Developed Vetting (DV).

3.6.3 Secure development

Our service is developed using our secure SDLC framework, including threat modelling, code review, secure coding standards and automated security testing. Validating the effectiveness of our controls, our Security Engineering Division completes internal annual audits.

3.6.4 Identity and authentication

Ensuring only authorised users can access Sayari Map, we require user identification either via username or Single-Sign On via your Identity Provider.

In the event that access needs restricting, for example due to the completion of a contract, our Customer Success Team can restrict access. Providing support, clients benefit from 1-2-1 support from their dedicated CSM, who can organise restrictions to be applied to specific users or accounts.

3.7 Auditing

Comprehensive audit logs capture all significant user and system actions, including user activity and system events across application, network and database layers.

3.7.1 Performance monitoring and metrics

To deliver a high-quality service, we will implement a performance management framework that includes the following core elements:

- Establishing Key Performance Indicators (KPIs)
- Monitoring our performance
- Enforcing our processes
- Producing reports
- Managing failures
- Fostering continuous improvement

3.7.2 Compliance and quality management

Our services are delivered under a structured and integrated management system aligned with internationally recognised best practice standards. Performance data, customer feedback and audit findings are reviewed regularly to identify improvement opportunities and track corrective actions.

3.8 Backup, restore & disaster recovery

To safeguard all client and corporate information assets, we maintain comprehensive Data Protection, Business Continuity and Information Governance policies. Ensuring service continuity, data integrity and minimal disruption to client operations, our approach is fully aligned with UK GDPR, ISO 27001 and 27701.

Overview and governance

Our Business Continuity Management (BCM) framework identifies potential threats, evaluates their impact and defines structured response procedures. The Security Engineering division activates recovery protocols, coordinates communications and oversees service restoration. We conduct regular risk reviews and verify readiness, test technical resilience and evidence compliance.

Backup and data protection

- **Daily automated backups:** Customer data is encrypted and backed up nightly
- **Cloud replication:** Managed by our Cloud Infrastructure Division, systems are distributed across UK-based datacentres
- **Secure retention:** Backup media is encrypted in transit and at rest and stored in physically controlled facilities

Disaster recovery and restoration

In the event of disruption, our Disaster Recovery Plan sets out recovery priorities and escalation procedures.

Our defined objectives are to:

- Restore essential systems within **24 hours**
- Limit potential data loss to less than **1 business day**
- Maintain continuous communication with client contacts throughout recovery

Continuous improvement and assurance

Following every exercise or live incident, we complete a post-event review and integrate lessons learned into updated procedures. This cyclical improvement model strengthens resilience and maintains full compliance with ISO 22301 and G-Cloud 15 Call-Off Terms.

3.9 Training

As standard with all licenses, Sayari provides user onboarding, training and regular end-user workshops. Making sure our customers get the most out of the software, this training is delivered by each client's assigned CSM. Dedicated consultant-led training is also available, chargeable as per our pricing.

Sayari provides all clients with access to Connect, our dedicated portal and customer hub. To facilitate user enablement, education and impact, this provides a single customised collaborative workspace with targeted assets and resources. Allowing clients to access useful resources, Connect includes:

- Information packs on getting started and onboarding assets
- Self-paced Sayari Map tutorials
- Product and data details
- Product roadmaps, updates and forthcoming events
- Recent domain-specific reports

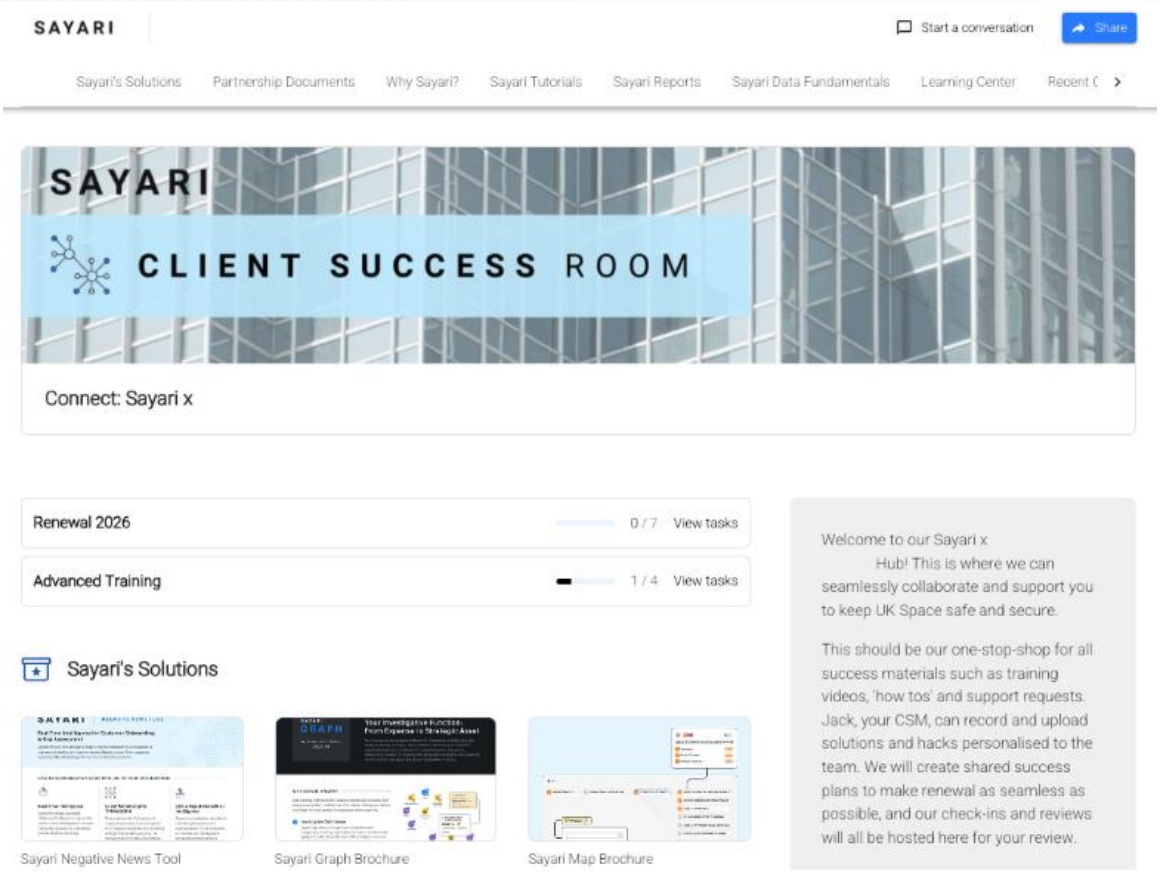


Figure 3.9.1: Sayari Connect

3.10 Service pricing

Sayari Map is available as an annual subscription model. Full pricing details are available within our Pricing File.

We provide free trial access to the Analyst Application (UI) with unlimited search and global data access. Free trials are typically granted for 1 to 2 month periods, with longer trials agreed on a case-by-case basis. Enabling our users to get the most out of our free trial, we provide onboarding and training sessions.

3.11 Invoicing process

Sayari's standard invoicing is on receipt of order, with payment terms of 30 days, in line with the government's standard 30-day payment terms.

3.12 Termination terms

Termination is governed by the Crown Commercial Service G-Cloud 15 Call-Off Terms and Conditions. The minimum contract term is 12 months. Buyers may terminate the contract in accordance with these terms by providing written notice 30 days prior to renewal. Sayari may terminate only in cases of material breach or non-payment. Upon termination, all data will be handled in line with our offboarding and data-deletion process described in Section 4.3.

4 Security and data governance

4.1 Data protection and encryption

To ensure the confidentiality, integrity, and availability of data, we apply robust encryption protocols to protect all sensitive data, both in transit, using TLS 1.2 or above encryption and AES-256 for data at rest. As a Cyber Essentials+ certified organisation, we follow best practices aligned with ISO 27001, ISO 27701 and National Cyber Security Centre guidance.

4.2 Data at rest, storage locations, and physical security

All data is stored within secure Google Cloud Platform UK data centres that comply with recognised security standards, including:

- CSA CCM V3.0
- SSAE-16/ISAE 3401

Safeguarding data at rest, these data centres provide robust physical access controls, such as monitored entry points, controlled access zones and continuous oversight.

4.3 Data sanitisation and disposal

Data sanitisation follows industry best practice, using cryptographic erasure or secure deletion techniques to ensure information cannot be recovered.

4.4 Security testing and assurance

For continued protection and resilience, we maintain a rigorous security testing and assurance programme. This includes annual penetration testing by Sapphire, an external NCSC CHECK-accredited organisation. Maintaining strong security controls, we review all findings and remediate promptly.

Providing continued assurance, we conduct ongoing monitoring, vulnerability scanning and regular reviews of our access controls and configurations.

4.5 Incident and protective monitoring management

Handling any potential security or service issues promptly, we operate a clearly defined incident management process. We can provide a copy of this upon request, which serves as evidence of our robust security and data governance measures.

Maintaining service integrity and continuity, all users can report incidents to their CSM, who then escalates this to Security through our internal procedures. Each incident triggers the creation of a formal incident report, documenting actions taken, outcomes and any required follow-up measures. Ensuring transparency, these reports are shared with all relevant internal and external stakeholders.

4.6 Configuration and change management

Making sure our infrastructure is developed securely, we maintain a robust configuration and change management framework. Providing full accountability, version control and controlled change processes, source control and development workflows are managed through GitHub Enterprise. Enabling consistency and validation before deployment, services operate on Kubernetes, with infrastructure defined and maintained as code. Minimising security risk, access to source code is strictly limited to authorised Sayari personnel whose roles explicitly require it.

Providing oversight, all significant changes are security-assessed before release.

4.7 Information security management and certifications

Evidencing the strength of our governance framework and third-party validation, we:

- Are accredited to SOC 2 Type 2, ISO 27001, ISO 27701 and Cyber Essentials+
- Complete annual internal audits
- Conduct annual penetration testing, completed by Sapphire
- Have an internal Security Engineering Team and Data Protection Officer

4.8 Secure development and cryptography

Embedding security considerations at every stage, we follow our structured SDLC approach. Ensuring all code changes meet our quality and risk requirements, we complete peer review, automated testing and security validation. Maintaining confidentiality and integrity, we implement cryptographic controls in line with industry best practice.

4.9 Identity and access management

Ensuring only authorised users can access Sayari Map, we require user identification. Managing access, we use strong authentication options, including supporting SSO with the customer's Identity Provider. In the event that access needs to be removed, we can restrict access. Providing support, clients benefit from 1-2-1 support from their dedicated CSM, who can organise restrictions to be applied to specific users or accounts.

5 Supplier information

5.1 About us

Sayari is a risk intelligence provider that equips intelligence professionals with immediate visibility into complex commercial relationships. To do this, we deliver the largest commercially available collection of corporate and trade data from more than **250** jurisdictions globally. With over **10** years of experience, we are trusted by Fortune 500 companies, financial institutions and government agencies.

Supporting **7400** users in over **35** countries, we aim to empower both public and private sectors with a comprehensive, evidence-based model of global commercial relationships. Our platform enables confident decision-making in regulatory compliance, supply chain management and complex investigations into global networks and illicit activity.

5.2 Relevant experience and testimonials

Trusted as a partner to global government organisations across Defence and National Security, Law Enforcement and Government Departments, Regulators and Critical National Infrastructure, we have provided testimonials below.

Testimonials:

"Sayari's clear and evidence-based risk factors allowed Microsoft's investigators to quickly understand risk and communicate this to their supply chain partners."

"Sayari helped Google fill significant coverage gaps in key markets, including India, Brazil, Japan."

"Sayari's product blueprints reduced the signal-to-noise ratio by 57%, which became a key narrative in our pitch."

5.3 How to buy

Sayari's services can be procured directly through the CCS G-Cloud 15 Digital Marketplace. Buyers can search for Sayari on the Digital Marketplace and select the required service listing.

Once selected, the buyer and Sayari will:

1. Raise a Call-Off Contract under the G-Cloud framework terms
2. Issue a Purchase Order (PO) to confirm commencement

Ensuring transparency and compliance with public-sector procurement regulations, all engagements are delivered in line with G-Cloud framework conditions.

Enquiries or pre-contract discussions can be arranged through:

- Email: sayari_ukpublicsector_gcloud@sayari.com