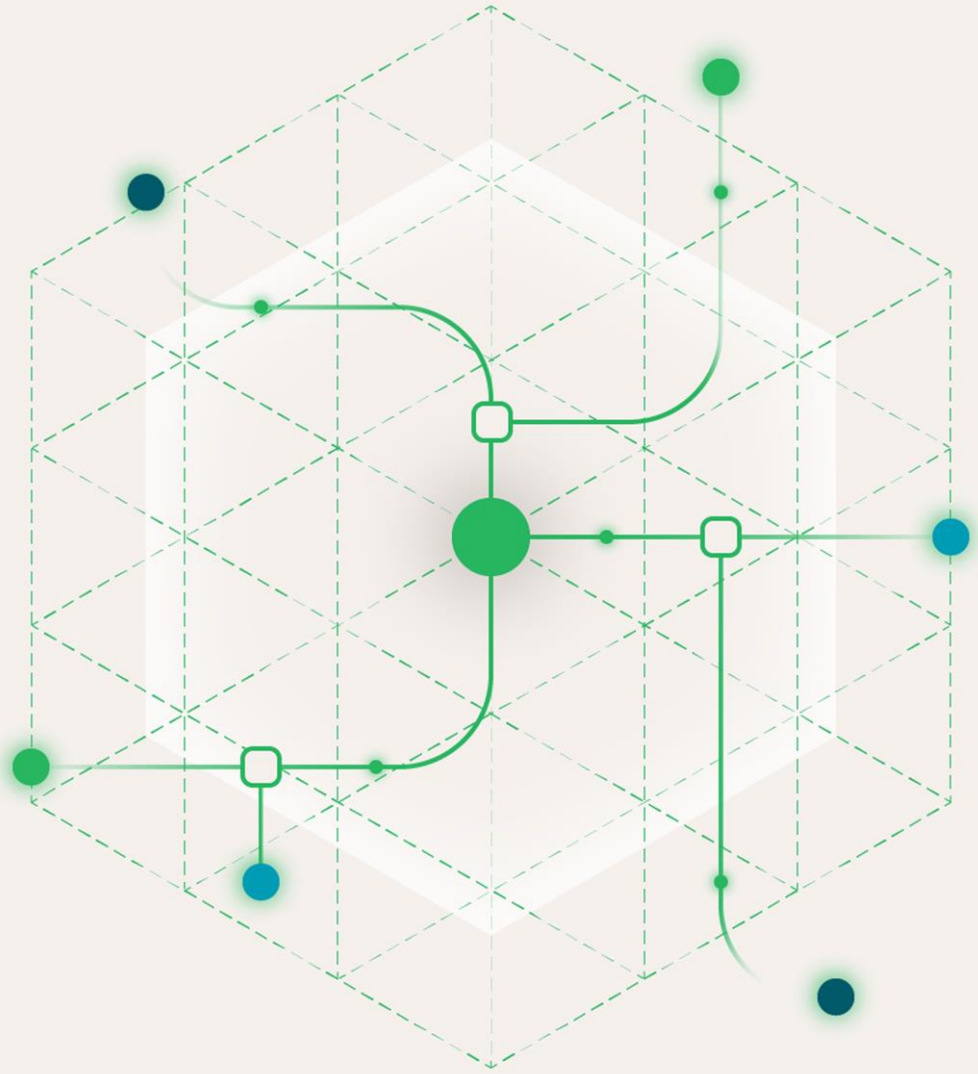
SYNECTICS SOLUTIONS



SERVICE DEFINITION

Sonar

Synectics Classification: Public

Classification Status: Public

In the UK, please contact:

Synectics Solutions
Hamil Road
Burslem
Stoke-on-Trent
ST6 1AJ

Tel: 0333 234 3409

Synectics Solutions website: http://www.synectics-solutions.com

Document Information	
Document Owner	Jake Harley
Effective Date	14/04/2022
Last Reviewed Date	27/01/2026
Next Review Date	27/01/2027
Classification	Public

Document Control				
Date	**Issue**	**Name**	**Details**	**Sign-off**
27/01/2026	V2	Jordan Roberts	G-Cloud 15	

CONTENTS

1 EXECUTIVE SUMMARY

Sonar is an ongoing customer risk monitoring service delivered by Synectics Solutions. It enables organisations to continuously reassess the risk profile of existing customers, supporting compliance with anti-money laundering and financial crime obligations.

Customer risk can change over time as new information becomes available or as behaviour evolves across multiple products. Sonar provides periodic rescreening of back-book customers and consolidates risk indicators into a single, central view, enabling organisations to identify emerging risks and take proportionate action.

2 SERVICE OVERVIEW

Sonar extends the principles of onboarding screening into the lifecycle of an existing customer relationship. While initial checks may indicate low risk at onboarding, subsequent activity or newly shared intelligence may materially change that assessment.

The service rescreens customer data at agreed intervals and applies configurable rules to identify changes in risk. Results are presented through structured workflows that support investigation, escalation and auditability.

Sonar primarily uses data from the National SIRA fraud signal-sharing network and can be supplemented with additional third-party or internal data sources to support broader compliance and risk monitoring requirements.

3 CORE SERVICE CAPABILITIES

3.1 ONGOING RISK MONITORING

Sonar supports periodic monitoring of existing customers, including:

- Rescreening against new or updated fraud intelligence
- Identification of changes in customer risk over time
- Consolidation of risk signals across multiple products or accounts

Screening frequency is configurable to align with an organisation's risk appetite and regulatory framework.

3.2 RULES AND WORKFLOW MANAGEMENT

The Sonar rules engine is fully configurable, allowing organisations to:

- Define monitoring rules and risk triggers
- Route referrals into tailored investigative workflows
- Record actions and outcomes for audit and compliance purposes

Additional features such as watchlists and diary functionality support investigator control and case management.

3.3 DATA SOURCES AND INTEGRATION

Sonar's primary data source is National SIRA, the UK's largest cross-sector fraud signal-sharing network. The service can also ingest data from a range of third-party intelligence providers and internal systems, subject to agreement and additional cost where applicable.

This approach enables organisations to consolidate multiple monitoring obligations into a single service.

4 KEY BENEFITS

- **Operational Efficiency:** Reduces duplicate effort by providing a consolidated view of customer risk across products and teams.
- **Regulatory Support:** Helps organisations evidence ongoing customer monitoring and proactive financial crime controls.
- **Flexible Data Ingestion:** Supports the use of multiple intelligence sources to meet evolving compliance requirements.
- **Configurable Monitoring:** Allows rules, workflows and investigation tools to be tailored to organisational needs.

5 SERVICE DELIVERY AND SUPPORT

5.1 IMPLEMENTATION AND ONBOARDING

Implementation of Sonar is supported by a dedicated Project Manager who will:

- Manage the project plan and onboarding activities
- Lead system configuration and deployment
- Support production roll-out
- Deliver training to operational users

The service is configured in line with the customer's monitoring requirements and data landscape.

5.2 SUPPORT AND SERVICE LEVELS

Sonar is delivered as a hosted service supported by Synectics Solutions. Support arrangements and service levels are aligned with standard Synectics operational support models and are agreed during onboarding.

6 TECHNICAL OVERVIEW

6.1 ACCESS AND SECURITY

Sonar is a secure, web-based service accessible via modern browsers. Secure communication is enforced using encrypted connections, and access is restricted to authorised users.

Network and access controls are applied to ensure that only approved organisations and users can access the service.

6.2 DATA PROCESSING

Customer data is typically ingested via batch uploads and screened against agreed rule sets. Batch frequency is configurable and commonly aligned to monthly monitoring cycles, though alternative frequencies can be supported to meet specific risk requirements.

Screening results are generated by matching customer records against new or updated intelligence held within National SIRA and other configured data sources.

7 DATA SECURITY AND ASSURANCE

Synectics Solutions operates a formal Information Security Management System aligned with ISO/IEC 27001.

The organisation is committed to:

- Protecting information against unauthorised access
- Maintaining confidentiality, integrity and availability of data
- Meeting applicable regulatory and legislative requirements

Information security controls, risk management activities and periodic risk assessments are maintained to ensure ongoing compliance with recognised good practice standards.

8 SUPPORT AND SERVICE MANAGEMENT

Synectics Solutions provides ongoing support for its services to ensure availability, performance and continuity in line with agreed service levels.

8.1 SUPPORT AVAILABILITY

Standard application support is available:

- Monday to Friday, 07:00–19:00 (UK time)
- Excluding public holidays in England and Wales

Support services are delivered in accordance with ITIL-aligned service management practices. Services are actively monitored, and incidents are managed using structured processes to ensure timely restoration, effective communication and appropriate escalation. Where required, incident summary reports and root cause analysis are provided, and outcomes are used to drive continuous service improvement.

Extended support hours, including out-of-hours and weekend support, can be agreed on request, subject to commercial and service agreement.

8.2 ACCOUNT MANAGEMENT

All customers are provided with a dedicated account team, which typically includes a Client Success Manager, Service Delivery Manager and Account Development Manager.

This team acts as a trusted extension of the customer's fraud and financial crime function and supports:

- Ongoing optimisation of the service
- Alignment of service configuration with business objectives
- Strategic planning, benchmarking and roadmap development
- Industry collaboration and knowledge sharing

This engagement model ensures customer requirements are reviewed on a continual basis and that services evolve in line with operational and regulatory needs.

9 DISASTER RECOVERY AND BUSINESS CONTINUITY

Synectics Solutions maintains a formal disaster recovery and business continuity framework designed to ensure service continuity, data protection and controlled recovery in the event of a major incident.

9.1 RECOVERY ARCHITECTURE

Services are delivered from a primary UK-based private cloud environment, supported by a separate secondary disaster recovery environment.

Data and system components are protected through backup and recovery mechanisms aligned to the following standard recovery objectives:

- Recovery Time Objective (RTO): 48 hours
- Recovery Point Objective (RPO): 24 hours

Improved RTO and RPO targets can be agreed on request, subject to service scope and commercial agreement.

9.2 DISASTER RECOVERY PROCESS

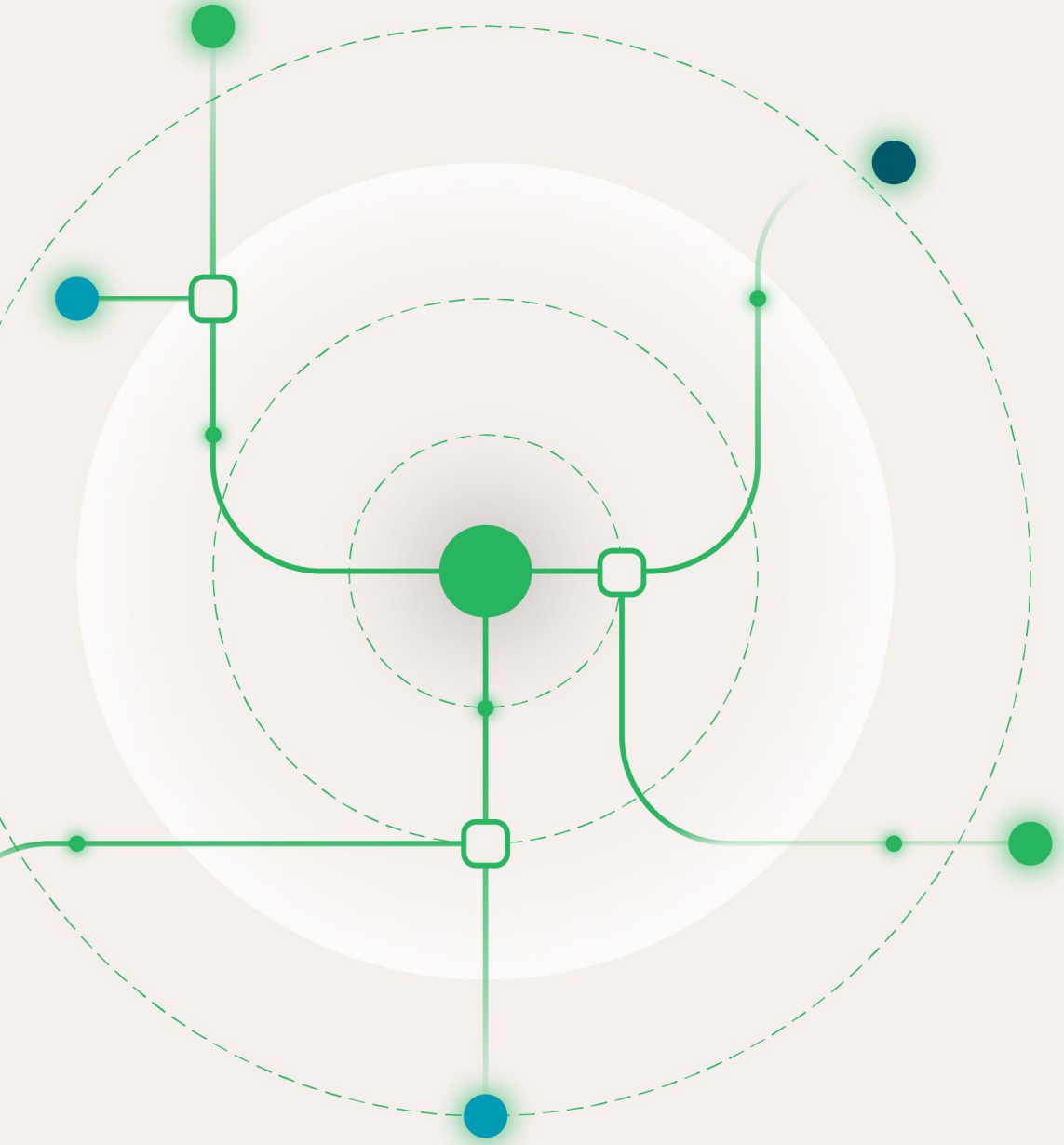
In the event of a critical service failure, documented procedures are followed to:

- Assess the nature and impact of the incident
- Invoke disaster recovery controls where required
- Restore services using the secondary environment and available backups
- Validate system integrity and data consistency prior to resuming normal operations

Recovery activities are governed by documented runbooks, clear escalation paths and defined roles and responsibilities to ensure a controlled and auditable response.

9.3 TESTING AND GOVERNANCE

Disaster recovery procedures are tested periodically to ensure effectiveness and operational readiness. Test outcomes are reviewed and used to strengthen resilience, refine recovery processes and support continuous improvement of the overall service.



SYNECTICS SOLUTIONS