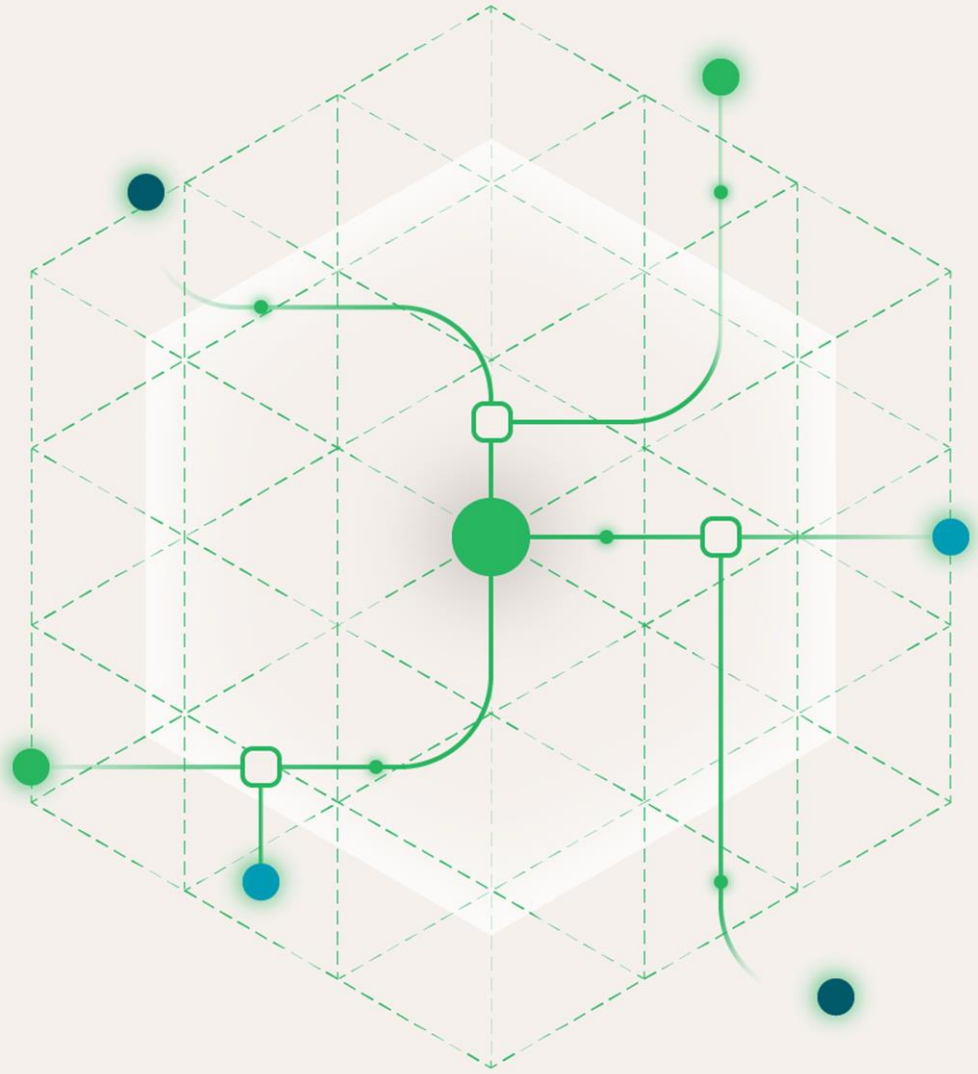
SYNECTICS SOLUTIONS



SERVICE DEFINITION

SIRA (Shared Intelligence for Risk Assessment)

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**
14/04/2022	V1	Mark Haslam	G-Cloud 12	
14/04/2022	V2	Liese Rushton	G-Cloud 13	
27/01/2026	V3	Jordan Roberts	G-Cloud 15	

CONTENTS

1 EXECUTIVE SUMMARY

SIRA is the UK's largest cross-sector fraud signal-sharing service, hosted and operated by Synectics Solutions Ltd. It enables organisations to identify potential fraud and inconsistency by matching customer enquiries against a nationally shared intelligence dataset.

The SIRA network comprises over 200 participating organisations across banking, insurance, telecommunications and consumer finance, with a dataset containing hundreds of millions of records. The service overlays this shared intelligence with a configurable rules engine, allowing incoming applications or customer events to be assessed in real time or batch processing modes.

Synectics Solutions has operated data-sharing and fraud prevention services since 2004 and has supported the identification of significant fraud and error savings across both public and private sectors.

2 SERVICE OVERVIEW

SIRA is a rules-based matching service that allows organisations to screen new applications, account updates or other customer events against previously shared risk indicators.

When an enquiry is submitted, SIRA evaluates the data using a combination of matching and behavioural rules. Where relevant matches or risk indicators are identified, the enquiry can be referred for further investigation by the customer organisation. Following review, the organisation records an outcome status which may contribute to future matching.

Records are retained in accordance with defined retention periods:

- Records marked as fraudulent or inconsistent are retained for up to six years.
- Records assessed as clear are retained for up to two years.

SIRA can be consumed as a real-time service, a batch service, or a hybrid of both, depending on customer requirements.

3 CORE SERVICE CAPABILITIES

3.1 MATCHING AND RULES ENGINE

SIRA supports multiple methods of risk detection, including:

- **Direct Matching:** Matching against previously recorded adverse indicators to identify known or suspected fraud risk.
- **Validation Rules:** Identification of high-risk data patterns where fraud has not been confirmed but risk indicators are present.
- **Velocity Rules:** Detection of unusual frequencies or patterns of activity that may indicate emerging fraud behaviour.

Rules can be configured to align with an organisation's specific risk appetite and customer journey.

3.2 RECIPROCITY AND DATA SHARING

SIRA operates as a reciprocal data-sharing service. Participating organisations are expected to contribute back to the network by marking enquiries as adverse where fraud or material inconsistency has been confirmed, subject to appropriate internal evidence and governance.

This reciprocal approach supports the collective identification of serial or cross-sector fraud while ensuring that only verified and proportionate information is shared.

3.3 NATIONAL FRAUD INITIATIVE (NFI)

Synectics Solutions hosts the National Fraud Initiative (NFI) on behalf of the UK Government. NFI data is held separately from SIRA and is owned and governed by the Cabinet Office.

Where permitted, and subject to separate agreement and cost, access to selected NFI datasets for the specific purpose of fraud prevention may be arranged directly with the Cabinet Office. Synectics Solutions can support customers by facilitating discussions where a suitable public-private use case exists.

4 KEY BENEFITS

- **National Intelligence:** Access to one of the UK's largest shared fraud intelligence datasets, spanning multiple sectors.
- **Flexible Integration:** Designed to integrate into existing customer journeys and decisioning processes, with configurable rules and workflows.
- **Scalability:** Suitable for organisations of varying sizes, supporting high-volume enterprise use cases through to lower-volume deployments.
- **Near Real-Time Decision Support:** Capable of delivering sub-second responses for real-time screening, supporting both manual review and automated decisioning.

5 SERVICE DELIVERY

5.1 IMPLEMENTATION AND ONBOARDING

Each implementation is supported by a dedicated Project Manager who will:

- Provide system integration documentation
- Coordinate onboarding activities
- Support user acceptance testing and production deployment
- Deliver training for operational and technical users

Implementation approaches are tailored to customer requirements and technical environments.

5.2 SERVICE LEVELS

SIRA is delivered as a highly available hosted service.

- Service availability: minimum 99.0%
- Planned maintenance:
    - Scheduled outside UK core business hours (07:00-20:00)
    - Typically no more than 3 hours per month for infrastructure maintenance
    - Software releases typically no more than 3 hours per quarter

6 TECHNICAL OVERVIEW

SIRA supports both real-time and batch processing models, including hybrid approaches.

6.1 REAL-TIME INTEGRATION

Real-time screening is provided via web services hosted by Synectics Solutions, enabling integration with customer systems using standard protocols:

- HTTPS
- REST
- SOAP

Responses can include structured indicators such as matched records, rules triggered and overall risk assessment, enabling the customer process to continue, pause, or route for review.

6.2 BATCH PROCESSING

Batch submissions are supported for overnight or intraday processing. Data transfer methods may include, for example:

- SFTP
- Managed file transfer solutions
- Secure network connections (e.g. IPsec VPN)

Batch frequency and timing are agreed during implementation and can be adapted to support near real-time use cases where required.

7 DATA SECURITY AND ASSURANCE

7.1 INFORMATION SECURITY MANAGEMENT

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
- Providing information security training to staff
- Reporting and investigating actual or suspected security incidents

Risk management and periodic risk assessments are undertaken to address changes in security requirements and operating environments. Independent certification is maintained through external audit.

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

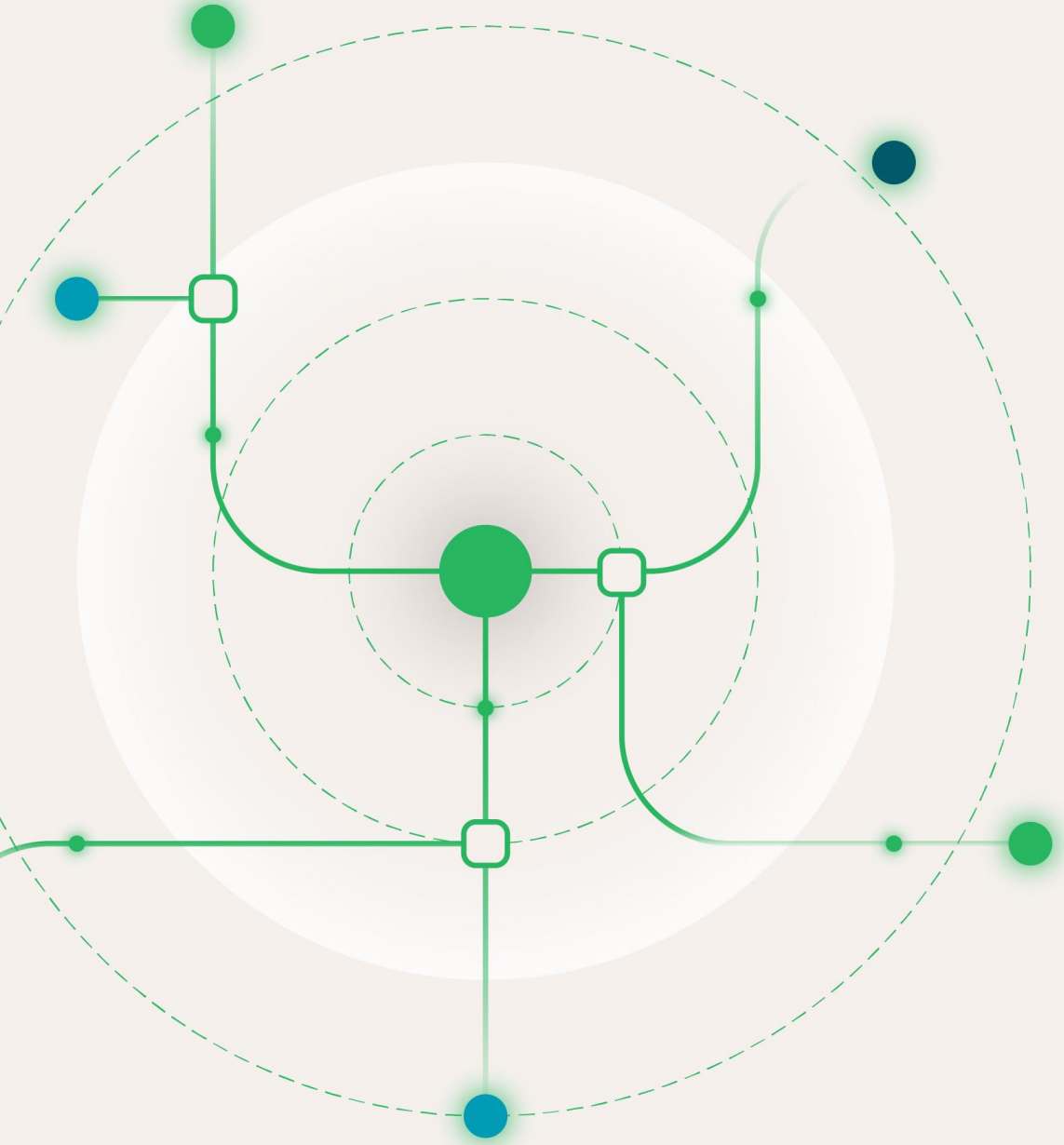
In the event of a critical service failure, documented procedures are followed to:

- 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