



Strider Technologies Limited

G-Cloud 15 Service Definitions Document (UK)

Lots covered:

- Lot 2b – Cloud Software (SaaS)

1. What the Service Is

Strider Technologies provides a **specialist cloud software service** designed to help organisations understand and assess security, compliance, and reputational risks associated with state-sponsored activity. The software analyses large volumes of open-source and difficult-to-access information and presents structured intelligence relating to people, organisations, technologies, and communications.

The service is delivered as **software-as-a-service (SaaS)** and accessed via a secure web application and APIs. Customers do not manage or configure infrastructure.

The service includes the following functional components, which may be licensed individually or together:

- People Search
- Organisations Search
- Insights
- Requests for Information (RFIs)
- Shield
- Strategic Intelligence Platform (including Spark)

2. How the Software Works

People Search

People Search enables users to review intelligence relating to individuals in order to identify potential risk indicators derived from open-source intelligence and Strider datasets. It supports due diligence, recruitment-related checks, and investigative workflows.



Organisations Search

Organisations Search supports third-party due diligence by identifying ownership structures, supplier and customer relationships, and links between organisations and restricted or high-risk entities.

Insights

Insights aggregates multiple risk indicators into structured views focused on an organisation's personnel, technologies, and external relationships. Dashboards and analytical views support prioritisation and review.

Requests for Information (RFIs)

RFIs provide written intelligence summaries relating to people, organisations, or topics of interest. RFIs may be analyst-assisted or AI-assisted, depending on customer configuration.

Shield

Shield is a curated intelligence dataset of email addresses, domains, and keywords associated with state-sponsored risk. It is provided via API for integration with existing security tooling.

Strategic Intelligence Platform (including Spark)

The Strategic Intelligence Platform provides a unified interface for accessing Strider software. Spark allows users to query available data using natural language and receive structured summaries based on licensed datasets and, where enabled, customer-provided information.

3. Data Backup, Restore, and Disaster Recovery

The service operates on a resilient cloud architecture. Controls include:

- Automated backups of production systems
- Encrypted backup storage
- Redundancy across multiple availability zones

Strider maintains documented **business continuity and disaster recovery procedures**, including defined recovery objectives. Backup and recovery processes are tested periodically.



4. Onboarding and Offboarding

Onboarding

Onboarding support typically includes:

- User account provisioning
- Introductory training sessions (remote)
- User documentation and guidance
- API onboarding support where applicable

Offboarding

On service termination, Strider supports:

- Deactivation of user access
- Export of customer-provided data where contractually agreed
- Secure deletion of customer data in line with retention obligations

5. Service Constraints

- The service is provided as a standard SaaS offering
- Configuration is limited to options available within the software
- Bespoke development is not included
- Planned maintenance is scheduled to minimise service impact

6. Service Levels

Availability

The software is designed for continuous operation and is generally available 24/7, excluding planned maintenance.

Performance



Performance depends on query complexity and data volume. The service is designed to return results in a timeframe suitable for operational use.

Support Hours

Support is provided during UK business hours. Enhanced support options may be available by agreement.

7. After-Sales Support

After-sales support includes:

- Technical support via helpdesk
- Ongoing customer success engagement
- Optional analytical and advisory services

8. Technical Requirements

Customers require:

- A modern, supported web browser
- Internet connectivity
- For API use, the ability to authenticate and consume RESTful APIs

No local software installation is required.

9. Outage and Maintenance Management

Planned maintenance is communicated in advance where possible. Unplanned incidents are managed through established incident management procedures, with customer communications provided as appropriate.



10. Hosting and Data Location

The software is hosted in secure cloud environments managed by Strider. For UK G-Cloud customers, data hosting and processing locations are aligned to UK and/or approved regions, subject to contractual and regulatory requirements.

11. Access to Data on Exit

On request and subject to contract, customers may:

- Receive an export of customer-provided data in a commonly used format
- Receive confirmation of secure deletion of customer data

Data is retained only as required to meet legal, regulatory, and contractual obligations.

12. Public Sector Use Cases

The Strider software supports a range of lawful public sector activities where specialist risk assessment software is required, including:

- **Third-party and supplier due diligence** to inform procurement, grants, and partnership decisions
- **Research and innovation security** to support publicly funded research and collaboration risk assessments
- **Recruitment and access screening support** alongside existing HR and security controls
- **Investigative and compliance support** by providing contextual external intelligence
- **Cyber and information security enrichment** through integration with existing security tooling

These use cases are illustrative and do not replace statutory, HR, or disciplinary decision-making processes.



13. Security

The service applies proportionate technical and organisational security controls, including:

- Role-based access control
- Encryption of data in transit and at rest
- Secure authentication mechanisms
- Monitoring and vulnerability management

The software is designed to support UK public sector security and data protection requirements, including UK GDPR where applicable.

