Strider Technologies Limited

G-Cloud 15 Service Definitions Document (UK)

Lots covered:

- **Lot 1a – Cloud Hosting (Platform support elements)**
- **Lot 2a – Cloud Software**

1. What the Service Is

Strider Technologies provides a **cloud-based Strategic Intelligence Platform** that enables organisations to identify, assess, and understand security, compliance, and reputational risks associated with state-sponsored activity. The service processes large volumes of open-source and difficult-to-access data 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. It does not require customers to install or manage infrastructure.

The G-Cloud service includes the following components, which may be used independently or together:

1. People Search
2. Organisations Search
3. Insights
4. Requests for Information (RFIs)
5. Shield
6. Strategic Intelligence Platform (including Spark)

2. Service Scope by G-Cloud Lot

2.1 Lot 2a – Cloud Software

Under Lot 2a, Strider provides application-level software that allows users to:

- Search and review intelligence on people and organisations
- View structured risk indicators and contextual information
- Generate reports and intelligence outputs
- Integrate intelligence into existing workflows via APIs

The software is accessed through a browser-based interface and APIs and is maintained and updated by Strider.

2.2 Lot 1a – Cloud Hosting (Platform Support)

Under Lot 1a, Strider provides the underlying **cloud platform services** required to host, operate, and secure the application. This includes:

- Cloud infrastructure management
- Data storage and processing environments
- Platform resilience, backup, and recovery

Customers do not directly manage hosting resources; these are operated by Strider as part of the managed platform.

3. How the Service Works

People Search

People Search enables users to query individuals to identify potential risk indicators based on open-source intelligence and Strider datasets. It supports due diligence, recruitment screening, and investigative workflows.

Organisations Search

Organisations Search enables due diligence on companies and institutions by identifying ownership structures, supplier and customer relationships, and links to restricted or high-risk entities.

Insights

Insights provides structured views that aggregate risk indicators related to an organisation's personnel, technologies, and external relationships. Information is presented in dashboards and analytical views to support prioritisation and review.

Requests for Information (RFIs)

RFIs provide written intelligence summaries on specific people, organisations, or topics. RFIs may be analyst-assisted or generated using AI-assisted tooling, depending on customer configuration.

Shield

Shield provides a curated dataset of email addresses, domains, and keywords associated with state-sponsored risk. It is delivered via API for integration with security tooling such as SIEM or DLP platforms.

Strategic Intelligence Platform (including Spark)

The Strategic Intelligence Platform provides a single interface to access Strider services. Spark enables users to query data using natural language and receive structured summaries based on available datasets and, where enabled, customer-uploaded information.

4. Data Backup, Restore, and Disaster Recovery

Strider operates a cloud-native architecture designed for resilience. The service includes:

- 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.

5. Onboarding and Offboarding

Onboarding Support

Onboarding typically includes:

- User account setup and access configuration
- Introductory training sessions (remote)
- Documentation and user guidance

- API onboarding support where applicable

Offboarding Support

On exit, Strider supports:

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

6. Service Constraints

- The service is provided as a standard SaaS offering
- Customisation is limited to configuration options provided within the platform
- Bespoke development is not included
- Planned maintenance is scheduled to minimise impact on UK business hours

7. Service Levels

Availability

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

Performance

Response times vary depending on query complexity and data volume. The service is designed to return results in a timely manner suitable for operational use.

Support Hours

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

8. After-Sales Support

After-sales support includes:

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

9. 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.

10. Outage and Maintenance Management

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

11. Hosting Locations

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

12. 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

Strider retains data only as required to meet legal, regulatory, and contractual obligations.

13. Public Sector Use Cases

The Strider service is designed to support a range of UK public sector use cases where understanding external security, compliance, and reputational risk is required. Typical use cases include:

- **Third-party and supplier due diligence:** Supporting assessments of suppliers, partners, grantees, or collaborators by identifying ownership structures, key personnel ties, and links to restricted or high-risk entities.
- **Research and innovation security:** Assisting publicly funded bodies, research organisations, and universities in identifying potential risks associated with collaborations, funding arrangements, or access to sensitive research and technology.
- **Recruitment and access screening:** Providing contextual intelligence to inform decisions about access to sensitive systems, data, or facilities, alongside existing HR and security processes.
- **Insider risk and investigations support:** Enabling security, compliance, and legal teams to better understand external relationships relevant to internal investigations, without replacing internal decision-making or statutory processes.
- **Cyber and information security enrichment:** Integrating curated intelligence into existing security tooling (such as SIEM or DLP systems) to support monitoring, investigation, and policy development.

These use cases are illustrative, and the service can be configured to support other lawful public sector risk-assessment activities.

14. Security

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