



Service Definition – What Caused This

1. Service overview

The service is a cloud-hosted Software as a Service (SaaS) platform that supports structured digital Root Cause Analysis (RCA). It enables organisations to collaboratively investigate incidents, identify root causes, share learning, and monitor trends across teams and sites.

The service is hosted in the UK and accessed through a web browser.

2. What the service does

The service provides a secure, web-based environment for conducting Root Cause Analysis using configurable investigation workflows. Users can capture evidence, document contributing factors, assign and track actions, and generate investigation reports.

The service includes real-time dashboards and geospatial visualisations to support analysis of incident patterns, recurring root causes, and organisational risk trends.

3. Service features

Key features include:

- Collaborative digital RCA workflows
- Configurable investigation templates and data fields
- Role-based access control and permissions
- Multi-factor authentication and single sign-on
- Web-based access via modern browsers
- Real-time dashboards with interactive filters
- Geospatial hotspot visualisation of incidents and RCAs
- Automated reporting and data export
- Secure REST API for system integration
- UK-hosted cloud infrastructure

4. Service benefits

The service enables organisations to:

- Identify root causes more quickly and consistently
- Improve collaboration across teams and locations
- Share learning from incidents across the organisation
- Gain visibility of trends and systemic risks
- Reduce investigation effort through structured workflows
- Support governance, audit, and assurance activities
- Improve consistency of RCA practices
- Support distributed and remote teams
- Scale usage as organisational needs grow
- Maintain secure access aligned with public-sector expectations

5. Users

The service is suitable for users involved in incident investigation, governance, and assurance activities, including:

- Operational staff conducting investigations
- Managers reviewing incidents and actions
- Governance, risk, quality, or compliance teams

Users access the service through a web browser. No specialist hardware or software is required.

6. Service delivery

The service is delivered as a subscription-based SaaS offering and is accessed remotely via the internet. The supplier manages hosting, maintenance, updates, and security.

Service enhancements and updates are deployed without requiring action from users.

7. Security and data hosting

The service is hosted on UK cloud infrastructure using Microsoft Azure UK regions. All service data is stored and processed within the UK.

Access to the service is protected using role-based access control, multi-factor authentication, and single sign-on via industry-standard protocols using Microsoft Entra ID. Data is encrypted in transit and at rest. Audit logging is enabled.

The supplier maintains an information security management system certified to ISO/IEC 27001 and holds UK Cyber Essentials certification. The service is designed to support UK GDPR compliance.

8. Support and onboarding

UK-based, human-led support is provided during UK business hours, Monday to Friday, 9am to 5pm. Support requests can be made via telephone or electronic channels.

The supplier provides onboarding support, including online training and user documentation, to help organisations configure the service and onboard users.

Support outside business hours may be available by prior agreement and may be chargeable. On-site support can be provided on request and is chargeable.

9. Integrations and interoperability

The service provides a secure REST API to support integration with existing systems. The API enables programmatic access to platform functionality, including data export.

API access uses industry-standard authentication and authorisation mechanisms, including OAuth bearer tokens. Role-based permissions are enforced consistently across the platform and API. API endpoints are documented using standard OpenAPI documentation. Rate limiting and IP controls are applied to protect service availability.

10. Service constraints and assumptions

- Internet access is required to use the service
- Users require a modern web browser
- Configuration is limited to available system options
- The service supports digital RCA activities only
- API usage is limited to documented endpoints and rate limits
- Support outside business hours is subject to prior agreement and additional charges
- On-site support is provided on request and charged separately