Service Definition – Citadel

---

1. Service Overview

Citadel is a cloud-hosted risk, compliance, assurance, and emergency planning platform that enables organisations to identify, assess, manage, and monitor strategic and operational risks, preparedness, and resilience in a structured and auditable way.

The service supports risk management, control assurance, emergency planning, training, and continuous improvement through configurable assessments, control mapping, emergency plans, exercises, and evidence tracking, all delivered via a secure, browser-based interface.

Citadel is provided as **Cloud Software (SaaS)**. No on-premise installation or customer-managed infrastructure is required.

---

2. Who the Service Is For

Citadel is designed for use by:

- UK public sector organisations
- Arm's-length bodies and public authorities
- Organisations with statutory or operational resilience, emergency planning, or compliance responsibilities

Typical users include senior management, risk and compliance teams, emergency planning officers, business continuity leads, internal audit functions, and operational managers who require clear visibility of risk exposure, preparedness, and control effectiveness.

---

3. What the Service Does

Citadel provides the following core capabilities:

Risk and Control Management

- Creation and management of strategic and operational risk libraries

- Definition, reuse, and mapping of control libraries
- Configurable assessments and question sets
- Automated scoring and aggregation of assessment results
- Centralised risk registers derived from assessment outcomes

Emergency Planning and Preparedness

- Creation and management of emergency and incident response plans
- Support for multi-agency or multi-site emergency planning structures
- Version-controlled plans with audit history
- Evidence capture to demonstrate preparedness and plan validation

Training and Exercises

- Integrated training modules linked to risks, controls, and plans
- Support for tabletop exercises, simulations, and post-incident reviews
- Tracking of training completion and exercise outcomes
- Evidence and audit trail to demonstrate organisational readiness

Evidence and Assurance

- Centralised evidence storage linked to risks, controls, assessments, and plans
- Full audit trail of changes, reviews, and approvals
- Reporting and dashboards to support governance, assurance, and oversight

Access and Governance

- Role-based access control and permissions
- Segregation of duties between administrative and operational users

All functionality is delivered through the standard Citadel service without bespoke development.

---

4. AI-Enabled Capabilities

Citadel includes AI-assisted features designed to support, not replace, human decision-making.

AI capabilities include:

- Assistance in structuring and reviewing risk statements and controls
- Support for generating draft assessment questions and guidance

- Analysis and summarisation of assessment outcomes and evidence

AI features operate within defined service boundaries and are used to augment user workflows. Final decisions, approvals, and risk ownership remain with the customer.

---

5. Service Model and Delivery

Citadel is delivered as a **fully managed cloud service**:

- Accessed via a standard web browser
- Hosted on secure cloud infrastructure
- No local software installation required
- Updates, improvements, and security patches are applied centrally by the supplier
- Customers access the service on a subscription basis

The service supports multiple environments (for example, testing and production) where required.

---

6. Onboarding and Configuration

Citadel is provisioned following order confirmation.

Onboarding includes:

- Creation of the customer environment
- Configuration of user roles and permissions
- Assistance with the setup of risk, control, assessment, emergency planning, and training structures
- Optional import of customer data using supported formats

All configuration is performed within the documented capabilities of the service. Citadel does not require bespoke development to operate.

---

7. Security and Data Protection

Citadel is designed with security and data protection as core principles.

Key measures include:

- Encryption of data in transit and at rest
- Role-based access control and secure authentication
- Logical separation of customer data
- Regular backups and monitored availability
- Secure session and access management

Citadel supports compliance with UK GDPR and relevant data protection legislation. Data is processed solely for the purpose of delivering the service.

---

8. Support and Service Management

Support is included as part of the service.

This includes:

- User support during agreed support hours
- Incident and fault management
- Access to user guidance and documentation
- Ongoing maintenance, updates, and service improvements

Support relates to the operation and use of the Citadel service and does not include consultancy or bespoke advisory services.

---

9. Service Constraints and Assumptions

- Internet access and a modern web browser are required
- The service is delivered within documented configuration parameters
- Customers are responsible for managing their users and permissions
- The service can be used offline

---

10. Data Portability and Exit Management

Citadel supports data portability.

At contract end or on request:

- Customer data can be exported in commonly used formats (for example CSV or structured files)

- Data can be retained for an agreed period