



G-Cloud 15

Service Definition Document:

Certify Health

Overview of the Service

Certify Health is a cloud-based assurance, compliance, and certification management service designed to help organisations plan, manage, evidence, and monitor compliance activities in a structured and auditable way. The service supports organisations operating in regulated and public sector environments by providing a central system of record for assurance processes, assessments, controls, and evidence.

Certify Health is delivered as Software-as-a-Service (SaaS) and accessed via a standard web browser. No local installation is required.

What the Service Is

Certify Health provides a configurable platform for managing certification and assurance activities, including compliance assessments, control frameworks, evidence collection, and reporting. The service enables organisations to track compliance status over time, manage remediation actions, and demonstrate assurance to internal and external stakeholders.

The service is designed to support a range of assurance use cases, including regulatory compliance, internal governance, supplier assurance, and quality management.

How the Service Works

Authorised users access Certify Health to define assurance frameworks, assessments, controls, and evidence requirements. The service supports structured workflows for assessment, review, approval, and remediation.

Certify Health maintains audit trails of user activity and changes to assurance records, supporting transparency and accountability. The service is maintained and updated by Santegic, with updates deployed without customer intervention.

Data Backup, Restore, and Disaster Recovery

Certify Health includes automated data backup processes designed to protect customer data against loss or corruption. Backups are stored securely and retained in line with documented retention policies.

Business continuity and disaster recovery arrangements are in place to support restoration of the service within defined recovery objectives following a major incident. These arrangements are reviewed and tested periodically.

Onboarding and Offboarding Support

Onboarding support includes initial service setup, configuration guidance, user access provisioning, and access to documentation. Optional training or assisted onboarding may be provided where agreed.

Offboarding support includes the ability to export customer data in a commonly used, machine-readable format upon request. Following service termination and any agreed retention period, customer data is securely deleted or anonymised.

Service Constraints

Certify Health is a standardised cloud service. Configuration is provided through the service interface; bespoke development or custom code changes are not included as part of the service.

Planned maintenance may be required periodically and is scheduled to minimise disruption where possible. Customers are notified in advance of planned maintenance.

Service Levels

Certify Health is designed to meet availability and performance expectations appropriate for an assurance management service. The service has a target availability of 99.9%, excluding planned maintenance.

Support is provided during standard business hours, with response targets based on incident severity, as described in service documentation.

After-Sales Support

After-sales support is provided via a service desk for incident reporting, service requests, and general enquiries. Customers have access to documentation and guidance to support ongoing use of the service.

Periodic service reviews may be conducted to ensure the service continues to meet customer requirements.

Technical Requirements

Certify Health requires:

- A modern, supported web browser
- Internet connectivity

Where integrations are required, these are supported through documented APIs, subject to third-party system availability.

Outage and Maintenance Management

The service is monitored to detect outages or performance degradation. In the event of an unplanned outage, customers are informed as soon as reasonably practicable, with updates provided until resolution.

Planned maintenance activities are communicated in advance wherever possible.

Access to Data on Exit

Upon exit from the service, customers may request a copy of their data in a commonly used, machine-readable format. Access to the service is removed following contract termination, and data is securely deleted in accordance with documented retention and deletion policies.

Security

Security is embedded in the design and operation of Certify Health. The service includes:

- Encryption of data in transit and at rest
- Role-based access controls
- Activity logging and audit trails
- Ongoing monitoring and security patching

Certify Health aligns with recognised information security standards and good practice, supporting customer compliance obligations.