



G-Cloud 15 Service Definition FMIS Equipment Maintenance (CMMS)

Version: 1.0

Date: January 2026

Classification: PUBLIC

Contents

1. Service overview3

2. Core functionality4

3. Access and interfaces5

4. Data import and export5

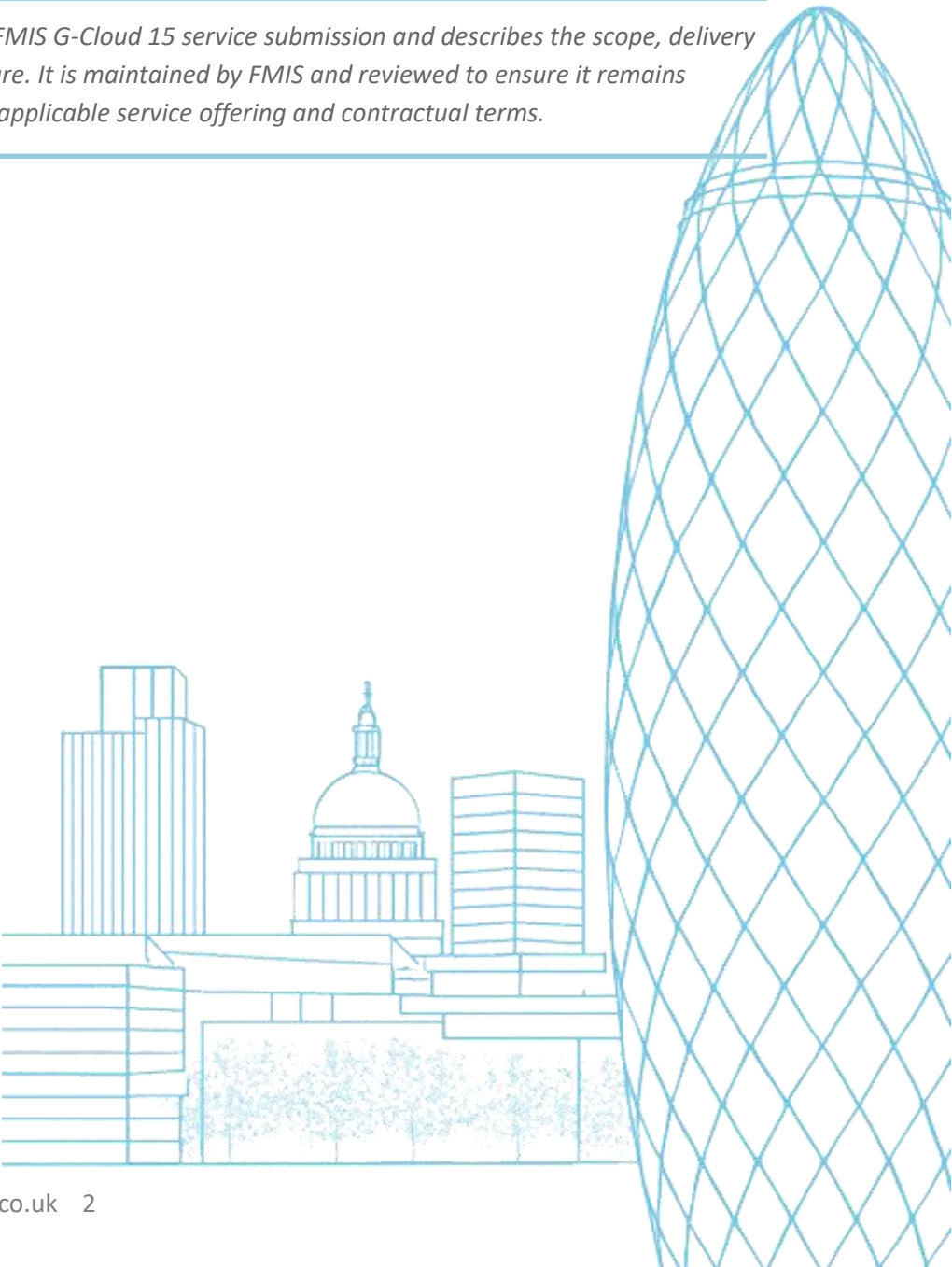
5. Support and onboarding6

6. Availability and resilience7

7. Security and governance7

8. Offboarding and exit8

This document forms part of the FMIS G-Cloud 15 service submission and describes the scope, delivery and operation of the FMIS Software. It is maintained by FMIS and reviewed to ensure it remains accurate and consistent with the applicable service offering and contractual terms.



1. Service overview

Service name

FMIS Equipment Maintenance (CMMS)

Lot

G-Cloud 15, Lot 2b – Software as a Service (SaaS)

Service description

FMIS Equipment Maintenance (CMMS) is a cloud-hosted, browser-based software service that enables organisations to manage equipment, maintenance activities and work orders. The service supports preventive and reactive maintenance, providing visibility of equipment condition, maintenance history and operational status to support uptime, compliance and audits through clear reporting and secure controls.

The service is delivered as a centrally managed SaaS solution hosted and operated by FMIS. No client-side software installation is required.

Intended users

The service is designed for organisations that require structured, auditable management of equipment maintenance activities. Typical users include facilities, estates, engineering, operations, health and safety and audit teams within public sector bodies, not-for-profit organisations and commercial entities.

Service scope

The FMIS Equipment Maintenance (CMMS) service includes:

- Centralised equipment and maintenance register
- Preventive maintenance scheduling (time-based and usage-based)
- Reactive maintenance and fault logging
- Work order creation, assignment, tracking and completion
- Maintenance history and service records per equipment item
- Equipment identification using unique IDs and barcodes
- Reporting to support maintenance oversight and audits
- Secure browser-based access
- Optional API access, enabled on request

The service supports equipment volumes ranging from hundreds to over one million records. This represents a capability statement rather than a contractual guarantee.

Delivery model

- Cloud-hosted SaaS
- Accessed via a standard web browser
- Hosted and managed by FMIS
- Public cloud or private cloud deployment options
- No client-side software installation required for standard browser access

Service options and extensions

The FMIS Equipment Maintenance service may be provided with additional options or related modules where required. These are not included as standard and may be supplied under a separate agreement.

Deployment options

The service is primarily delivered as a cloud-hosted SaaS solution managed by FMIS. On-premise deployment or client-managed hosting may be supported where required, subject to technical and commercial agreement.

Bespoke development

Bespoke configuration or development may be undertaken by FMIS where agreed in advance. Any such work is scoped, priced and contracted separately from the standard service.

Related FMIS modules

FMIS Equipment Maintenance can be used alongside other FMIS modules, including FMIS Asset Tracking, FMIS Fixed Asset Management and FMIS Lease Accounting. These modules are separate and are not included unless explicitly licensed.

2. Core functionality

FMIS Equipment Maintenance (CMMS) provides functionality to support the management, scheduling and control of equipment maintenance throughout the operational lifecycle.

Equipment register

- Centralised register holding equipment identifiers and descriptive data
- Configurable equipment fields and classification structures
- Support for multiple organisations, locations and departments
- Tracking of equipment ownership, responsibility and status
- Document and file attachments stored against equipment records
- Full audit history of equipment and maintenance actions

Maintenance scheduling

- Preventive maintenance schedules based on time, usage or meter readings
- Automatic generation of planned maintenance work orders
- Configurable maintenance frequencies and task templates
- Visibility of upcoming, overdue and completed maintenance

Work orders and fault management

- Manual and automated work order creation
- Logging and tracking of faults and reactive maintenance requests
- Assignment of work orders to users or teams
- Status tracking from creation through completion
- Recording of actions taken, dates and outcomes

Barcode and identification support

- Support for unique equipment identifiers
- Barcode-based equipment identification
- Barcode scanning supported via compatible mobile devices
- Rapid equipment verification during inspections and audits

Reporting and audit

- Standard and configurable reports covering maintenance activity and history
- Reporting on work orders, schedules and equipment status
- Search and filtering across equipment and maintenance records
- Export of reports to spreadsheet and PDF formats
- Audit logs available to authorised users, covering both FMIS and customer actions

3. Access and interfaces

User access

- Secure access via a standard web browser
- No client-side software installation required
- Role-based access control to restrict functionality and data by user role
- Customer administrator users can manage users and permissions within the service

User interface

- Web-based user interface designed for desktop and laptop use
- Mobile browser access supported with reduced functionality compared to desktop access
- Accessibility features supported through standard browser functionality, including zoom and keyboard navigation

Audit access

- Authorised customer administrator users can view audit logs directly within the service
- Audit logs include both customer and FMIS actions, subject to user permissions
- Audit information is available during normal system operation

4. Data import and export

Data import

FMIS Equipment Maintenance provides tools to support the import of equipment and maintenance-related data into the service.

- Import of equipment and maintenance data using structured templates
- Primary import format is CSV
- Spreadsheet formats, including Excel (XLSX), supported where required
- Import processes support bulk creation and update of equipment records
- Data migration supported as part of onboarding, led by FMIS consultants

Data export

Customers can export their data from the service at any time.

- Export of equipment and maintenance data in CSV or spreadsheet formats
- Export of reports in PDF format
- Data can be exported during the contract term and at end of contract
- No restrictions on customer access to their own data

Application programming interface (API)

FMIS provides an application programming interface (API) to support integration and data access for FMIS Equipment Maintenance.

- API access is optional and not enabled by default
- API access is enabled by FMIS on request and controlled via system configuration and user permissions
- The API supports retrieval of equipment and maintenance-related data
- The API is not used for initial system provisioning or full system administration
- No separate sandbox or test environment is provided
- API documentation is available in HTML format

5. Support and onboarding

Support model

Standard support for FMIS Equipment Maintenance is included within the service licence.

- Support is provided by FMIS during UK business hours
- Support channels include email and telephone
- Support requests are prioritised and managed by FMIS
- There is no customer-controlled ticket prioritisation
- No dedicated Technical Account Manager or named support resource is provided as standard
- Third parties engaged by the customer may access support where authorised

Support availability

- Standard support hours are 09:00 to 17:00 UK time, Monday to Friday
- UK public holidays are excluded
- Support outside standard hours is not provided unless separately agreed

Onboarding

Onboarding is delivered remotely and led by FMIS consultants.

- Structured onboarding process tailored to customer maintenance requirements
- Configuration of the system to align with operational maintenance processes
- Data migration support using standard import tools
- Remote training provided for customer users and administrators
- User documentation provided in accessible digital formats

Ongoing service delivery

- Software updates and fixes are managed and deployed by FMIS
- Changes are assessed and controlled through FMIS change management processes
- Customers are notified of relevant updates where appropriate

6. Availability and resilience

Service availability

- FMIS Equipment Maintenance has a target availability of 99.9% per calendar month
- Availability excludes scheduled maintenance and permitted downtime, as defined in the Licence Agreement
- Availability targets are measured across the service as a whole
- Any service credits or remedies are governed by the applicable agreement

Hosting and resilience

- The service is hosted in a managed data centre environment
- Hosting includes resilient power, connectivity and environmental controls
- Infrastructure is monitored and managed by FMIS and its hosting partners
- Redundancy is designed to reduce the risk of single points of failure

Backup and recovery

- Regular backups are performed as part of the service
- Backup and recovery processes are designed to support service continuity
- Recovery procedures are tested and maintained as part of operational governance

Business continuity and disaster recovery

- Business continuity and disaster recovery arrangements are in place
- Arrangements align with FMIS information security and continuity policies
- Plans are designed to support recovery following significant service disruption
- Further detail can be provided to customers on request

Outage communication

- There is no public service status dashboard
- Customers are notified of significant service outages by email
- Communications are provided where appropriate based on impact and duration

7. Security and governance

Information security governance

- FMIS operates an information security management framework aligned with ISO/IEC 27001
- Security governance is overseen by the FMIS Data Protection and Information Security Lead
- Security policies cover access control, incident management, change management, supplier security and business continuity
- Governance arrangements are reviewed and maintained as part of ongoing operations

Data protection

- Customer data is processed in accordance with applicable data protection legislation
- Logical access to customer data is restricted to authorised users and FMIS personnel
- Access is granted on a least-privilege basis

Network and infrastructure security

- Data in transit is protected using TLS 1.2 or higher
- Internal network protections include layered controls such as segmentation, firewalls and access controls
- Hosting environments are managed by third-party providers aligned with recognised security standards

Data at rest

- Data stored within the service is protected using encryption and logical access controls
- Storage media protections are managed as part of the hosting environment

Data sanitisation

- Formal data sanitisation processes are in place
- Data erasure and cryptographic erasure methods are used where appropriate
- Physical destruction or degaussing is not claimed for cloud-hosted environments

Change and vulnerability management

- Changes are assessed, approved and tracked through supplier-defined change management processes
- Security impact is considered prior to implementation of changes
- Vulnerability management is risk-based
- Threat intelligence is informed by vendors, hosting providers and recognised advisories
- Patching is prioritised based on severity rather than fixed timelines

Protective monitoring and incident management

- Monitoring is in place to identify system activity and anomalous behaviour
- Documented incident management procedures are followed
- Customers can report incidents via standard support channels
- Updates and summary information are provided where appropriate
- No fixed incident response time guarantees are stated

Personnel security

- Staff are subject to appropriate screening processes
- Government clearances are held where required for specific roles
- All FMIS staff, data centres and offices are based in the United Kingdom

8. Offboarding and exit

Data access and export

Customers retain access to their data throughout the contract term and during the offboarding process.

- Customers can export their data at any time using standard export tools
- Data can be exported in CSV or spreadsheet formats and PDF
- API access, where enabled, may be used to retrieve data prior to exit

End of contract

- At contract end, customers are responsible for exporting their data from the service
- No exit fees apply for standard offboarding
- FMIS does not require customers to purchase an archive or extended access service as part of exit

Data deletion

- Following contract termination and completion of offboarding, customer data is removed from the service
- Data deletion is performed in line with FMIS data sanitisation processes
- Deletion activities are governed by information security and data protection policies

Offboarding support

- Reasonable assistance is provided to support customer offboarding
- Additional support beyond standard offboarding may be provided by agreement