



Driving Secure Digital Transformation

GCloud 15

Secure UK Gitlab as a Service

January 2026

Secure UK Gitlab as a Service

Summary

Secure UK GitLab as a Service provides a UK-hosted, supplier-managed GitLab cloud software service for public sector organisations.

The service enables secure source code management, collaboration, and continuous integration/continuous delivery (CI/CD) within a secure UK-sovereign environment, helping organisations improve software delivery while reducing the operational burden of managing GitLab infrastructure.

Features

- UK-hosted GitLab platform operated as a managed cloud service
- Secure Git repositories with role-based access control
- Version control supporting standard Git workflows
- Integrated CI/CD pipelines for automated build, test, and deployment
- Merge requests to support structured code reviews and approvals
- Issue and task tracking integrated with code changes
- Built-in wiki functionality for project documentation
- Webhooks and APIs for integration with external systems
- Support for automated testing tools and pipeline extensions
- GitLab analytics and reporting features for visibility of development activity

Benefits

- UK data sovereignty supporting public sector assurance requirements
- Reduced operational overhead through supplier-managed platform operation
- Secure collaboration across internal teams and trusted delivery partners
- Improved delivery efficiency through automated CI/CD workflows
- Consistent tooling across development, test, and live environments
- Improved quality and traceability through integrated code review, testing, and issue tracking
- Flexibility to integrate with existing cloud platforms and delivery tooling

Service Description

This service delivers GitLab as a fully managed cloud software platform, hosted and operated within the UK. It provides core GitLab functionality including version control, CI/CD pipelines, issue tracking, code review, and documentation, with the supplier responsible for platform operation and lifecycle management.

The service supports modern software delivery practices by providing a consistent platform for managing source code and automating build, test, and deployment workflows across development, test, and live environments. GitLab can integrate with

existing infrastructure and tooling, including container-based application workflows, where required.

GitLab licences can be provided as part of the service or buyers may use licences they already hold. The digital marketplace pricing includes onboarding and configuration to align the platform with buyer requirements, while buyers retain control of repositories, users, permissions, and development workflows.

This service provides the cloud software platform only and does not include bespoke software development or consultancy unless separately procured.

Who the service is for

This service is suitable for public sector organisations that require a secure, UK-hosted GitLab platform without the need to operate and maintain GitLab infrastructure themselves.

It is appropriate for:

- Central government departments
- Arm's-length bodies
- Local authorities
- Public sector delivery partners

Security

The service uses GitLab's built-in security controls, including access management and encryption of data in transit and at rest where supported by the platform.

The platform is hosted within the UK to support data residency requirements. Access to the service is controlled through role-based permissions, and activity within the platform is logged for auditability.

Onboarding and offboarding

Onboarding includes initial configuration of the GitLab platform, user access setup, and support for migration of existing repositories where required.

On service termination, buyers can export repositories and data using standard GitLab tools.

Support

Incident Management

Viewdeck classifies incidents raised at its service desk using the following P1 – P3 priority. Incidents raised with the Service Desk will be triaged and responded to accordingly in priority order.

- P1 Total loss of service to all users.
- P2 Some loss of critical service for some or all users.
- P3 Limited loss of service or work around possible limiting loss experienced.

Priority	Response type (during standard business hours)	Target resolution (Mon-Fri 9-5)
P1	30 minute response, sustained effort using all necessary and available resources until service is restored.	4 hours
P2	4 hour response to assess the situation, staff may be interrupted and taken away from lower priority jobs.	1 working day
P3	One working day response using standard procedures and operating within the normal frameworks.	3 working days