Website: https://logit.io

Email: sales@logit.io

Logit.io Platform

UK G-Cloud 15 Framework

Service Definition Document

Issue Date: 20th December 2025

Version: 1.0

Points of Contact

Lee Smith

Logit.io Sales

lsmith@logit.io
sales@logit.io

11192-ISMS-001

HM Government G-Cloud Supplier

Table of Contents

Logit.io Platform

1. Introduction

This document describes the Logit.io Platform, which underpins multiple cloud services offered by Logit.io on the G-Cloud framework. It provides a common overview of platform capabilities, security controls, governance, service management, and operational processes that apply across all Logit.io services.

Individual service scope, features, limits, and pricing are defined in the relevant G-Cloud service listings.

2. Platform Overview

The Logit.io Platform is a cloud-hosted, fully managed observability platform that supports the collection, storage, search, and analysis of operational data, including logs, metrics, and trace data. The platform is designed to support operational monitoring, incident investigation, security analysis, and compliance reporting across cloud, hybrid, and on-premise environments.

The platform removes the need for customers to operate or maintain observability infrastructure by providing a centrally managed service delivered over the public internet.

3. Platform Capabilities

Platform capabilities include:

- Centralised collection and analysis of operational data
- Log management and search
- Metrics collection and visualisation
- Distributed tracing and application performance monitoring
- Dashboards and visualisations
- Alerting and notifications
- Audit logging of user actions

The platform supports modern cloud-native, containerised, hybrid, and on-premise data sources.

4. Service Delivery Model

The Logit.io Platform is delivered as a **public cloud, multi-tenant managed service**. Customers access the platform through a secure web-based interface and APIs.

Logit.io is responsible for platform operation, maintenance, monitoring, and security. The platform integrates with customer environments for data ingestion but does not require deployment into customer-owned infrastructure.

5. Security Governance

Logit.io operates an **ISO/IEC 27001–certified Information Security Management System (ISMS)**. Information security policies and procedures cover risk management, access control, incident management, change management, supplier assurance, and business continuity.

Security governance is overseen by senior management. Compliance is maintained through regular risk assessments, staff training, internal audits, penetration testing, and management review.

6. Identity and Access Management

Access to the platform is controlled using:

- Federated identity through SAML-compatible identity providers
- Multi-factor authentication enforced via the identity provider
- Role-based access controls
- Least-privilege access principles

Administrative access is restricted to authorised personnel. All access and administrative actions are logged for audit purposes.

7. Audit Logging and Monitoring

The platform records audit logs of user activity within management interfaces. Customers can access audit information in real time through the platform interface.

Audit data retention is configurable by the customer. Platform activity is continuously monitored to identify anomalous behaviour and potential security incidents.

8. Data Protection

Data at Rest

Customer data is encrypted at rest using industry-standard encryption. Encryption keys are managed and monitored in accordance with security policies.

Data in Transit

Data transmitted between customer systems and the platform is protected using Transport Layer Security (TLS) version 1.2 or higher.

Data Retention and Deletion

Customers define data retention policies for their services. At contract termination or service deletion, customer data is permanently deleted in line with the configured retention policy.

9. Data Portability and Exit

Customers can export their data prior to or at contract termination using supported APIs and snapshot and restore functionality. Data can be exported in open formats, including CSV, JSON, and plain text, as well as platform-compatible snapshot formats.

Assistance with data export and transition to another service can be provided at additional cost if required.

10. Resilience and Availability

The platform is designed for resilience using horizontally scalable components deployed across isolated infrastructure resources and multiple datacentre locations. Automated monitoring and recovery mechanisms detect failures and restore service operation.

Availability targets depend on the selected service and service package. Standard availability targets are defined in individual service listings and associated SLAs.

11. Incident Management

Logit.io operates defined incident management processes as part of its ISO/IEC 27001–certified ISMS. Pre-defined procedures exist for common incident types and severity levels.

Incidents can be reported through multiple support channels. Incident updates are communicated via a public service status page and, where appropriate, directly to affected customers.

12. Support and Onboarding

Customers are supported through:

- Guided onboarding via the platform interface
- Online documentation and help centre resources
- Email and ticket-based support
- Live chat support during published hours

Enterprise support options, including dedicated account management and priority technical support, are available for eligible services.

Optional onsite training and workshops may be provided at additional cost.

13. Configuration and Change Management

Platform configuration and change management are governed by the ISO/IEC 27001–certified ISMS. All changes undergo documented risk and security impact assessments and require approval before deployment. Changes are tested in non-production environments prior to release and monitored post-deployment.

14. Vulnerability and Protective Monitoring

The platform operates vulnerability management processes aligned with ISO/IEC 27001. Vulnerabilities are identified through scanning, penetration testing, and threat intelligence. Remediation is prioritised based on risk and severity.

Protective monitoring is performed continuously to detect potential compromises. Incidents are handled according to defined incident response procedures.

15. Business Continuity

Logit.io maintains and tests business continuity and incident response plans in line with ISO/IEC 27001 requirements. These plans are designed to support platform continuity and recovery in the event of disruptive incidents.

16. Customer Responsibilities

Customers are responsible for:

- Providing data sources with network connectivity

- Using supported web browsers
- Managing user identities through their chosen identity provider
- Configuring retention policies and access controls appropriate to their needs

17. Standards and Compliance

The Logit.io Platform operates in alignment with:

- ISO/IEC 27001 (Information Security Management)
- UK Government Cloud Security Principles
- Applicable data protection regulations

18. Relationship to G-Cloud Services

This Platform Service Definition applies to multiple Logit.io services listed on the G-Cloud framework. Individual service descriptions define specific functionality, limits, service levels, and pricing.