



IDAM, Single Sign-On (SSO) Design, Integration, Support

SERVICE DESCRIPTION

*This service description forms part of a G-Cloud 15 service listing
Service Category: F-201-000-000 (Managed Cloud)*

JANUARY 2026

Who We Are

About the Supplier



We are a UK-based technology services provider specialising in cloud delivery and digital transformation for the public sector.

We support central government, arm's-length bodies, local authorities and not-for-profit organisations to transform business capabilities, services and processes through secure, well-governed cloud solutions.

Our teams bring deep technical, security and delivery expertise, with over 25 years of public sector experience across senior leadership, client and supplier roles.

This experience enables us to understand public sector operating environments and deliver user-focused outcomes that are practical, sustainable and aligned to organisational objectives.

What We Do

We provide cloud software and cloud support services to public sector organisations.

Our services support the digital transformation of business processes and systems, including the delivery of secure digital platforms, real-time asset monitoring and tracking solutions, and Zero Trust network architectures aligned to NCSC guidance.

We help customers design, implement, operate and improve cloud-based services with a focus on security, resilience, usability and value for money.

Service Capabilities



Public Sector Experience

We have experience delivering services to public sector organisations with varying security, scale and regulatory requirements.

Our teams understand public sector governance, assurance and procurement obligations, and tailor delivery to meet these needs.

Our staff bring senior consultancy and service delivery experience, including former senior civil service and executive-level roles. This background provides practical insight into public sector operating environments and enables us to support digital transformation initiatives that are well-governed, user-focused and aligned to organisational priorities.



Aligned to Best Practices

We design and deliver services using open standards and established best practices to improve service quality, support interoperability and reduce long-term cost.

Our services are aligned to the GDS Technology Code of Practice and are designed in line with NCSC security and architecture principles, supporting secure, resilient and well-governed public sector services.



Specialist Divisions

We operate specialist capability areas delivering professional services, cloud software and managed services.

These include DevOps and ServiceOps delivery, real-time asset monitoring and reporting solutions, and the operation of a global IoT data network supporting large-scale device deployments.

Our services support the secure management and monitoring of connected assets in complex public sector environments.

Delivery Capability and Scale

We combine focused specialist delivery with the breadth of capability required to support complex public sector services. Our size and structure enable us to respond flexibly to customer needs while maintaining the capacity, governance and resilience expected of a mature technology services provider.

Service Overview

Our Service



This service provides cloud software and/or cloud support activities to public sector customers. The service supports the design, implementation, operation and ongoing improvement of cloud-based solutions in line with Crown Commercial Service requirements.

Service Description

End-to-end identity and access management service covering design, integration, deployment, and operational support. Delivers secure Single Sign-On and adaptive MFA integrated with Microsoft Entra ID (Azure AD), Okta, and Office 365, enabling seamless user access, reduced risk, and compliant identity control across cloud, on-premise, and hybrid environments.

What Can It Do?

Features

1. NCSC-aligned IDAM design and integration
2. Single Sign-On (SSO) and adaptive Multi-Factor Authentication (MFA)
3. Industry-standard MFA implementation
4. Authentication via Active Directory, LDAP, ADFS, Okta
5. Integration with Microsoft Entra ID (Azure AD) and Office 365
6. SAML and API-based access management
7. B2B and partner identity integration
8. User provisioning and lifecycle management
9. Enterprise architecture, design, and disaster recovery support
10. Collaborative knowledge transfer to in-house teams

Benefits

1. Compliance with NCSC identity and access guidance
2. Seamless access from any device or location
3. Reduced security risk through strong authentication controls
4. Single credential access to multiple applications
5. Faster and more secure rollout of cloud applications
6. Reduced operational effort and support costs
7. Centralised management of cloud, on-premise, and mobile users
8. Enforced password and access policies
9. Improved user experience with fewer login challenges
10. Aligned with ISO 27001, 20000-1, 14001, 9001, Cyber Essentials Plus

Onboarding and Implementation

Onboarding is designed to be efficient and proportionate, with established processes to enable service initiation, requirements confirmation, access setup and initial configuration.

Delivery approaches are agreed with the customer to align with existing programmes and minimise disruption.

Our teams work using agile, multidisciplinary delivery methods to support timely mobilisation and effective implementation.

Service Initiation



Understand the Requirement

We work with customers to develop a clear understanding of service requirements, objectives and constraints. This enables us to assign resources with directly relevant experience and an appropriate level of seniority to support effective delivery.



Service Scope

The scope of the service is defined and agreed prior to delivery. This includes confirmation of deliverables, timescales, quality criteria and dependencies, alongside an understanding of customer constraints, sensitivities and key drivers. This approach ensures



Resourcing and Availability

Delivery is planned to ensure that appropriately skilled resources have committed availability for agreed activities. Resource allocation and delivery timescales are confirmed during service initiation to support predictable delivery and agreed



Review / Agree Engagement

Following initial discussions and planning, customers have the opportunity to review and refine the proposed engagement. This includes confirming scope, delivery approach and proposed resources. Where appropriate, introductory discussions can be arranged to ensure alignment and confidence before delivery begins.



Value-Focused Delivery

Based on prior delivery experience, we may suggest alternative solutions or additional areas of scope that could deliver improved outcomes or efficiencies over time, subject to customer agreement.

The process is highly consultative to ensure that you are fully aware of the exit plans. Off-boarding is managed through a structured and consultative process agreed with the customer. Where appropriate, this includes knowledge transfer and handover activities to support continuity of service. Off-boarding activities are delivered in line with the Call-Off Contract.

Ordering Process

How To Order



Public sector customers can order this service through the G-Cloud Digital Marketplace using the G-Cloud Call-Off Contract.

Following order placement, service scope, delivery approach and start dates are confirmed with the customer in line with the agreed service definition. Services commence on the agreed start date and are delivered in accordance with the Call-Off Contract and associated documentation.

Charges are applied in line with the published pricing document, using the agreed pricing model and units. Invoicing is typically monthly. Payment terms are 30 days from receipt of a valid invoice, in accordance with the Call-Off Contract.

Customer Responsibilities

Customers are responsible for providing timely access to relevant stakeholders, systems, information and approvals required to support service delivery. Any customer dependencies, such as inputs to review or assurance activities, are identified and agreed during service initiation to enable effective delivery.

Service Constraints

Constraints and Dependencies



The service operates within agreed customer policies, technical environments and security constraints. Dependencies on third-party platforms, customer readiness and access approvals may affect delivery timescales.

Security

Security and Assurance



Security is integral to service delivery. The service aligns with ISO 27001, ISO 20000-1, ISO 9001, ISO 14001 and Cyber Essentials Plus. Security responsibilities are shared between the Supplier, the Customer and relevant cloud service providers in line with the shared responsibility model.

Technical Requirements



Technical Prerequisites



Technical requirements are agreed with the customer and may include supported operating systems, cloud platforms, identity services and access controls. Customers are responsible for providing necessary access approvals.

Hardware

Hardware Considerations



Where hardware is required, it is ancillary to the cloud service and charged separately. Hardware requirements are confirmed during onboarding and may include customer-owned or supplier-managed components.



Data Access, Exit, and Offboarding



Data Management and Exit



Customer data remains the property of the customer at all times. On service exit, data will be returned or securely deleted in accordance with the Call-Off Contract. Exit support is available where required.

Pricing

Pricing and Charging



Pricing details are provided in the associated pricing document. Third-party licences, subscriptions, cloud consumption and hardware costs are excluded unless explicitly stated.



Document Control and Compliance



Document Control



This document is maintained under formal document control and complies with applicable legal, regulatory and G-Cloud framework requirements. This document forms part of a G-Cloud 15 service listing and is subject to the G-Cloud Framework Agreement and Call-Off Contract.

Service Levels

Service Level Approach



Service levels and support arrangements are agreed with the customer as part of the Call-Off Contract.

Support and After Sales Service

Ongoing Support



Ongoing support is provided throughout the service lifecycle, including incident management, service requests, advice and continuous improvement activities.

Backup, Restore, and Disaster Recovery

Backup and Recovery Approach



Backup, restore and disaster recovery responsibilities are defined in line with the shared responsibility model of the underlying cloud platforms. The service supports the configuration and validation of backup controls where applicable.

Outage and Maintenance Management

Incident and Maintenance Management



Planned maintenance and changes are communicated in advance where possible. Incidents and outages are managed using defined incident management processes, with updates provided until resolution.

Hosting and Service Locations

Hosting and Delivery Locations



Services are delivered using cloud platforms hosted in the UK or approved regions. Service delivery and support activities are provided from approved locations in line with public sector requirements.



Contact Details:

The Principle Point of Contact is:

Visionist Limited

1 Austin Park, Yeoman Road
Ringwood, Hampshire, BH24 3FG

t: 020 3883 8201

e: info@visionist.com



Crown
Commercial
Service
Supplier

Microsoft
Partner

okta



IASME Consortium®



© 2026 Visionist Limited

This document is the property of Visionist Limited. It shall not be reproduced in whole or in part, nor disclosed to a third party, without prior written permission. No responsibility or liability is accepted for any errors or omissions in this document or related documents.

Head Office:

1 Austin Park, Yeoman Road
Ringwood, Hampshire,
BH24 3FG

t: 020 3883 8201

e: info@visionist.com



Registered Office:

Merlin House
No. 1 Langstone Business Park,
Newport
NP18 2HJ

