



G-Cloud 15 Lot 3 – Cloud Support Services

Service Definition Document

Alasdair Murray
Chief Technology and Product Officer
Condatis

Document Control

Title	G-Cloud 15 Lot 3 – Cloud Support Services
Filename	Condatis.G-Cloud15.SDD.Lot3.Draft.docx
Author / Creation Date	Alasdair Murray / 13 January 2026
Version / Document Type	v[CalcVersion] / [Document Type]
Information Handling Classification	[Classification]

Distribution	Client
Document Owner	[Owner]
Review Due (DD/MM/YYYY)	
Review Approver	[Review Approver]
Publish Approver	[Publish Approver]

Client Name / Client Code	/
Project Name / Job Code	N/A

Revision History

Date	Author	Change
13 January 2026	Alasdair Murray	Draft
21 January 2026	Ian Stewart	Review
27 January 2026	SMT	Final Version

Table of Contents

1	Introduction.....	4
2	Pricing	4
3	Service Levels	5
4	Onboarding and Offboarding.....	5
5	User Support	6
6	Asset Protection and Security	7
7	Staff Security	8
8	Social Value Commitments	8
9	Accessibility & Inclusivity.....	9
10	Performance Metrics	9
11	Security Certifications	10
12	Case Study - DWP EAS system	11
13	Mapping to G-Cloud 15 Lot 3 Categories	12
14	Compliance Table	12
15	Terms & Conditions.....	13

1 Introduction

Condatis delivers expert Cloud Support Services under the G-Cloud 15 framework, specifically aligned with Lot 3 requirements. Our offering focuses on enabling public sector organisations to adopt, optimise, and manage secure identity solutions built on Microsoft Entra, AI and Azure technologies. Through a combination of strategic advisory, professional services, and managed services, we help clients achieve robust security, compliance, and operational efficiency.

We're defining support as both

- Traditional ongoing support or managed support services to existing identity-based systems to both maintain and extend those systems – this submission
- Prebuild support for organisation that need assistance in defining, architecting and creating and integrating Identity system into their organisations. This is dealt with in our Lot 2a services submission

Our services are designed to support organisations throughout the entire cloud journey, from initial planning and migration to ongoing optimisation and governance. Condatis extends Microsoft's native capabilities with tailored components and best-practice frameworks, ensuring seamless integration with existing systems and alignment with UK Government Cloud Security Principles.

Key elements of our Lot 3 service include support for :

- **Pre-existing Microsoft identity system support** – onboarding and supporting existing Microsoft identity system such as B2C, MIM, Entra ID Entra ID gov etc
- **Digital Identity Support / Managed Service:** ITIL-aligned support with proactive monitoring and rapid incident resolution.
- **Trusted Advisor Services:** Strategic guidance on identity governance, compliance, and risk management.
- **Delivery and Integration:** Expert implementation of Microsoft Entra solutions, including MFA, RBAC, and decentralized identity.
- **Transformation Readiness:** Assessments and roadmaps to prepare organisations for future identity models and regulatory changes.

Condatis is committed to delivering measurable social value, maintaining ISO/IEC 27001 and Cyber Essentials Plus certifications, and providing flexible pricing models to meet diverse organisational needs. Our UK-based team ensures responsive support and compliance with all G-Cloud standards.

2 Pricing

See separate sheet. We provide information on our mechanism to establish price and then provide outlines on the following

- Onboarding cost
- Baseline price for provision of the service options (as monthly unit price)
- Price certainty
- Prices for specific support option
- SflA Rate card if needed for support augmentation

3 Service Levels

Condatis guarantees high reliability and responsiveness through clearly defined Service Level Agreements (SLAs) aligned with G-Cloud standards:

- **Service Availability**
 - Uptime Guarantee: 99.9% monthly availability for core identity services hosted on Microsoft Azure.
 - Monitoring: Continuous monitoring with automated alerts for service degradation.
- **Incident Response**
 - Response Times:
 - Critical incidents: Initial response within 30 minutes.
 - High priority: Within 1 hour.
 - Standard issues: Within 4 business hours.
 - Resolution Targets:
 - Critical: Resolved within 4 hours.
 - High priority: Within 8 hours.
 - Standard: Within 24 hours.
- **Support Channels**
 - UK business hours support as standard.
 - Optional 24/7 coverage for critical environments.
 - Multi-channel support: Email, ticketing system, telephone, and web chat.
- **Escalation Procedures**
 - Documented escalation paths aligned with ITIL best practices to ensure rapid resolution of complex issues.
- **Performance Reporting**
 - Monthly reports covering:
 - Uptime statistics.
 - Incident response and resolution times.
 - SLA compliance metrics.
 - Regular service reviews and optimisation based on performance data.

These service levels ensure operational continuity, rapid incident resolution, and proactive performance management for all clients.

4 Onboarding and Offboarding

Condatis provides a secure, structured **onboarding** process to ensure rapid service readiness and minimal disruption:

- **Seamless Transition:** We enable controlled access and transfer of knowledge, including test suites, CI/CD pipelines, monitoring tools, and infrastructure responsibilities, ensuring continuity of service.
- **Integrated Support:** Helpdesk workflows are established and tested to deliver efficient ticket management across all parties.
- **Clear Governance:** Advance onboarding notifications (five working days) and prompt offboarding (within one day) maintain compliance and transparency. Regular progress updates and six-monthly service reviews underpin accountability.

- **Security Assured:** Access is role-based and aligned to least privilege principles, with MFA and Privileged Identity Management enforced. Our approach meets ISO 9001, ISO 27001, Cyber Essentials Plus, and ITIL standards.
- **Agile Delivery:** Onboarding follows an Agile framework with Sprint 0 for discovery and acceptance criteria, then iterative two-week sprints with demos and formal sign-off for predictable outcomes.
- **Comprehensive Documentation:** Governance artefacts such as PID, risk registers, and change logs ensure traceability and audit readiness.

Condatis ensures a secure, compliant, and efficient **offboarding** process to protect client assets and maintain service integrity:

- **Rapid Access Revocation:** All logical and physical access rights are removed promptly to prevent unauthorised activity and reduce any related license costs.
- **Account Deactivation:** User accounts across identity platforms (e.g., Entra ID) and service management tools are disabled or deleted in line with governance policies.
- **Asset Recovery:** Buyer-issued devices and credentials are returned and verified, ensuring no residual risk.
- **Knowledge Continuity:** Critical information is captured and transferred to maintain operational stability and avoid service disruption.
- **Compliance Assured:** Processes align with ISO 27001, ISO 9001, Cyber Essentials Plus, and ITIL standards, delivering audit-ready governance.
- **Immediate Offboarding Capability:** For high-risk scenarios (e.g., security breach), Condatis executes accelerated removal of access and assets under CxO and HR oversight.
- **Automated & Auditable:** Integrated workflows with Entra ID Governance and service desk systems provide full traceability and reporting for assurance.

5 User Support

Condatis provides end-to-end support and aftercare to ensure successful adoption and integration of Entra Identity solutions within client environments. Our support model is designed to deliver clarity, security, and operational efficiency throughout the engagement lifecycle.

Definition and Design

- **Discovery Workshops** - Collaborative sessions with client stakeholders to capture business objectives, compliance requirements, and technical constraints.
- **Solution Architecture** - Design of a tailored architecture leveraging Microsoft Entra and Azure technologies, ensuring interoperability and alignment with UK Government Cloud Security Principles.
- **Use Case Mapping** - Definition of user journeys, credential templates, and trust frameworks to meet organisational needs.

Integration and Deployment

- **Integration Planning** - Development of detailed migration roadmaps covering data transfer, configuration, and testing phases.
- **Custom Connectors** - Creation of connectors for legacy systems and hybrid environments to ensure seamless interoperability.

- Configuration and Orchestration - Implementation of workflows, role-based access controls, and silent issuance capabilities.

Hypercare Support, Duration and Scope

- Duration: Hypercare typically spans two to four weeks post-deployment or major transition, with flexibility based on project complexity and client requirements.
- Scope:
 - Dedicated support team available during extended hours.
 - Enhanced monitoring of identity services and integrations.
 - Daily status calls and rapid escalation paths for any issues.
 - Immediate remediation of defects and performance tuning.
 - Knowledge transfer sessions to ensure client teams are fully equipped for steady-state operations.

Ongoing Support Options

- **Retainer based or prepaid support**
 - UK business hours support via email and portal.
 - Call of support can be used for all Condatis roles to provide devops, architect or developer support for existing identity system
- **Standard Support**
 - UK business hours support via email and portal.
 - Defined SLAs for response and resolution times.
- **Enhanced Support**
 - Optional 24/7 coverage for critical environments.
 - Proactive monitoring: Leveraging Microsoft Azure Monitor and AI-driven analytics, we identify anomalies and potential failures before they impact service. Predictive alerts allow us to remediate issues proactively, reducing downtime and improving reliability. For example, identity service health indicators are tracked to forecast capacity or configuration risks.
- **Full managed service**
 - As above with all aspects of the service supported and maintained and updated by us and full integration with you existing support teams
- **Training and Knowledge Transfer**
 - Onboarding sessions for administrators and end-users.
 - Comprehensive documentation and best practice guides.
- **Continuous Improvement**
 - Condatis operates under an iterative improvement model, reviewing service performance monthly and implementing enhancements based on SLA compliance, incident trends, and client feedback. This includes regular updates to support processes and automation scripts to reduce resolution times.
 - Regular service reviews and optimisation based on performance data.
 - Advisory on emerging identity standards and compliance updates

6 Asset Protection and Security

Condatis ensures the highest standards of asset protection and security across all Lot 3 Cloud Support services. We are fully compliant with ISO/IEC 27001 and adhere to GDPR requirements for data privacy and protection. Our approach includes:

- **Encryption:** All data is encrypted in transit and at rest using industry-standard protocols.

- **Access Management:** Role-based access controls (RBAC) and multi-factor authentication (MFA) are implemented to prevent unauthorised access.
- **Vulnerability Management:** Regular vulnerability scanning and patching are conducted to maintain system integrity.
- **Penetration Testing:** Periodic penetration tests are performed to identify and remediate potential security risks.
- **Audit and Monitoring:** Continuous monitoring and audit trails ensure accountability and rapid detection of anomalies.

These measures guarantee that customer data and systems remain secure throughout the service lifecycle, from onboarding to offboarding.

7 Staff Security

Condatis applies rigorous security measures to ensure that all personnel involved in delivering Lot 3 Cloud Support services meet the highest standards of trust and compliance. Our approach includes:

- **Pre-Employment Screening:** All staff undergo comprehensive onboarding checks, including identity verification, employment history, and criminal record checks, in line with UK Government, Scottish Government and Digital Marketplace requirements. These checks are done to BS7858 standard
- **Security Clearances:** Where required by the Buyer or project scope, we ensure staff hold appropriate UK Government Security Clearances (e.g., SC, or DV). We currently have SC cleared staff and maintain the flexibility to meet higher clearance levels for sensitive engagements.
- **Continuous Compliance:** Staff are trained in data protection, ISO/IEC 27001 security principles, and GDPR compliance. Regular refresher courses and audits ensure adherence to best practices throughout the contract lifecycle.

This structured approach guarantees that only vetted and authorised personnel handle customer data and systems, reducing risk and maintaining confidence in service delivery.

8 Social Value Commitments

Condatis is committed to delivering measurable social value throughout the lifecycle of our services and software. Our approach aligns with the UK Government's Social Value Model and focuses on the following key themes:

- **Fighting Climate Change**
 - Condatis designs and operates services using GreenOps principles, optimising resource consumption and reducing carbon emissions through efficient use of Microsoft Azure cloud infrastructure and automation.
 - Commitment to net-zero targets by minimising energy usage and supporting sustainable hosting practices.
- **Tackling Economic Inequality**
 - Condatis only uses UK-based delivery teams, creating local employment opportunities and supporting regional economic growth.

- Offer skills development programmes for employees and clients, including training on identity security, cloud technologies, and compliance frameworks.
- **Equal Opportunity**
 - Condatis promotes inclusive recruitment practices, ensuring diversity and equal opportunity across all roles.
 - We provide accessible solutions compliant with WCAG and other UK Government standards to ensure usability for all users, including those with disabilities where required.
- **Wellbeing and Community Integration**
 - Support employee wellbeing through flexible working arrangements and mental health initiatives.
 - Engage with local communities via STEM outreach programmes and apprenticeships encouraging careers in technology and cybersecurity.

9 Accessibility & Inclusivity

Condatis is committed to ensuring that all services are accessible and inclusive for every user. Our approach includes:

- **Compliance with Accessibility Standards**
 - All user interfaces and documentation are designed to meet Web Content Accessibility Guidelines (WCAG) 2.1 AA standards and other mandated standards where and when required.
 - Regular accessibility audits are conducted, with clients, to maintain compliance and improve usability for individuals with disabilities.
- **Inclusive Design Principles**
 - Solutions are developed using inclusive design practices, ensuring compatibility with assistive technologies such as screen readers, voice recognition software, and alternative input devices.
 - Clear, consistent navigation and adaptable layouts support users with varying needs.
- **Language and Cultural Inclusivity**
 - Multi-language support is available for key service components.
 - Content is written in plain English to ensure clarity and ease of understanding.
- **Ongoing Improvement**
 - Accessibility feedback channels are provided for clients and end-users.
 - Continuous improvement processes ensure enhancements based on user feedback and evolving standards.

10 Performance Metrics

The support services will predominantly be based around SLA defined above in summary these would be as follows

Availability

- 99.9% monthly uptime
- < 45 minutes/month unplanned downtime

Responsiveness

- P1: respond 30 min, resolve 4 hrs
- P2: respond 1 hr, resolve 8 hrs

- P3: respond 4 hrs, resolve 24 hrs

Quality

- SLA compliance $\geq 98\%$
- First-time fix rate $\geq 70\%$
- Reopen rate $\leq 5\%$

Efficiency

- Average resolution time
- % automated or self-service resolutions

Stability & Reliability

- Release failure rate $\leq 2\%$
- Mean time between incidents (MTBI)
- Patching compliance 100%

These are provided as a starting point but other improved performance levels can also be discussed

11 Security Certifications

Condatis and Microsoft maintain rigorous security standards to ensure the confidentiality, integrity, and availability of client data. Our services comply with recognised industry certifications and frameworks, including:

Condatis	
ISO 27001	Yes
ISO 90001	Yes
Cyber Essentials Plus	Yes
GDPR	Yes
SOC1&2	
Secure Development Lifecycle	Yes
NIST 800-88	Yes
Penetration Testing	Where requested

12 Case Study - DWP EAS system

The Client

The Department for Work and Pensions (DWP) is responsible for welfare, pensions and child maintenance policy to around 20 million claimants and customers. It also provides information to around 20,000 local and central government users across 400 different networks



The Challenge

DWP had a need to replace the existing decommissioned multifactor authentication system with a suitable alternative. The transition would need to work with their existing physical tokens and be delivered with no downtime to their 20,000 users. In addition, several key enhancements were to be made to allow their users to 'self-serve' on several actions avoiding lengthy waits and a physical paper trail. The solution had to maintain service, improve performance and reduce costs with no loss of security.

The Solution

Condatis in conjunction with DWP architects and Microsoft produced an Azure B2C based solution written with a Microservices based architecture. The system runs on two UK data centres with failover between the two. Users are multifactor authenticated using their credentials and their physical Onespan token. Role based access controls (RBAC) provides a 5-deep hierarchy of administrative users with authentication and workflows allowing DWP to populate, protect and monitor access to the overall system and their respective services.

Seamless transition was managed progressively through the project using 'silent journeys' and intermediate steps to allow each local authority in turn to experiment and to validate their revised access prior to full adoption. Transition was phased over several months.

The Benefits

- The resulting system performed faster and in addition, users were impressed with the efficiency improvements produced by their ability to self-administrate previously centrally handled functions. The interface employed Government Digital Services (GDS) guidelines throughout and were found to be easy to use.
- Maintenance and control were improved by having the complete system under the secure control of DWP's own Azure subscription including all audit storage. This gave a larger sense of ownership than the previous solution. The project was delivered in an agile way using two week sprints.
- The system was and is extensible. The initial system provided local government access to three distinct services within DWP. A further two new services were added since go live with minimal additional work.

13 Mapping to G-Cloud 15 Lot 3 Categories

Condatis support services align with the award criteria defined under Lot 3 The following table illustrates how our solution meets these requirements:

G-Cloud Lot 3 Category	Condatis Alignment
Price	Condatis prices are designed to be competitive for the expertise we bring to a project and are outlined in a separate sheet
Social Value	Condatis is committed to delivering measurable social value throughout the lifecycle of our services and software, these are outlined in Social Value Commitments
User support	Condatis provides comprehensive user support under all aspects of Identity management and have a long history of doing so for public sector clients. The options for this provision are defined in User Support
Staff security clearance	All staff are vetted to BS7858 standards as defined in Staff Security
Staff security levels	A proportion of our delivery staff have SC level clearance as sponsored by various organisations
Cyber Essentials	Condatis have both Cyber Essential and Cyber Essential plus designations and ISO27001 and ISO9001

14 Compliance Table

Requirement	Condatis Compliance
User Support	UK business hours support via email, ticketing system, and telephone as standard; optional 24/7 coverage for critical environments; SLAs for response and resolution times; escalation procedures aligned with ITIL best practices.
Asset Protection	Data stored in UK/EU regions; ISO/IEC 27001 and GDPR compliance; encryption at rest and in transit; regular vulnerability scanning and penetration testing; audit trails for accountability.
Penetration Testing	Annual penetration tests by certified third parties where requested; remediation documented and tracked; aligned with NCSC and Secure Development Lifecycle guidance.
Data Sanitisation	Secure erasure using NIST 800-88 standards; ISO 27001-certified processes; audit trail provided for verification; optional migration support offered.

Security Certifications	ISO/IEC 27001, ISO 9001, Cyber Essentials Plus maintained throughout contract; GDPR compliance; Secure Development Lifecycle implemented.
Accessibility & Inclusivity	WCAG 2.1 AA compliance; inclusive design principles; multi-language support; accessibility audits and feedback channels for continuous improvement.
Social Value	Commitment to net-zero and GreenOps principles; inclusive recruitment and equal opportunity; STEM outreach and skills development programmes; support for employee wellbeing and community engagement.

15 Terms & Conditions

Standard G-Cloud terms apply. Additional terms specific to Condatis services will be provided upon request, covering SLAs, data protection, and compliance obligations.