



SERVICE DEFINITION G-CLOUD LOT 2: CLOUD SOFTWARE

Identity and Bank Ownerships Checks

Contents

1. Introduction.....	2
2. Company Overview.....	2
3. Service Description.....	2
4. Core Features & Functionality	3
5. Benefits.....	3
6. Maximising Impact – Synergistic Services	4
7. Service Constraints.....	4
8. Onboarding & Offboarding	5
9. Service Levels & Support.....	7
10. Technical Architecture	9
11. Information Security & Compliance	10
12. Data Protection.....	10
13. Pricing.....	13
14. Service Roadmap.....	13
15. Terms & Conditions.....	13
16. Existing Users	13
17. Ordering, Billing & Invoicing.....	14



1. Introduction

This Service Definition outlines the scope, features, deployment model, support model, pricing structure and compliance posture of this Service provided by Ascendant Solutions Limited under the G-Cloud Framework.

ID & Bank Ownership verification provides councils with a combined identity check and bank account ownership match, ensuring that a person's name, address, date of birth, sort code and account number align with verified credit bureau held data. It is used to validate applicants, detect fraud risk, confirm legitimate claimants, and identify mismatches early across Apply4.Online® workflows and related services.

2. Company Overview

Ascendant Solutions Limited is a multi-award-winning UK public-sector technology provider, recognised nationally for innovation, service quality and measurable impact across Revenues, Benefits and Housing services. The company has earned repeated IRRV Performance Awards across 2021, 2022, 2023 and 2025, including *Excellence in Innovation*, *Excellence in Debt Management*, and *Innovation in the Fight Against Poverty*.

In addition to its strong sector reputation and proven delivery record with Local Authorities, Ascendant Solutions achieved one of the highest honours available to UK businesses, the King's Award for Enterprise (Innovation). The award recognised our Apply4.Online® product following exceptional national uptake and significant contribution to public sector digital transformation.

3. Service Description

ID & Bank Ownership verification is a combined service that:

- Confirms identity by validating name, address, and date of birth against credit bureau sources.
- Verifies bank ownership by checking that a supplied sort code and account number belong to the individual.
- Returns a structured scorecard, indicating match/no match outcomes, confidence levels, and flags for fraud risk indicators.

It integrates directly within local authority business processes particularly fraud detection, financial assessment, grant eligibility, and income related applications. It is widely used within Apply4.Online® for DHPs, Household Support Fund (HSF) and the Crisis and Resilience Fund (CRF).



4. Core Features & Functionality

Identity Check

- Matches Name, Address, Date of Birth against bureau records.
- Provides corroboration outcomes (aligned / partial match / mismatch).
- Number of bankruptcy or insolvency records listed against the customer
- Number of CCJs listed against the customer

Bank Account Ownership Verification

- Confirms whether a supplied Sort Code + Account Number exists.
- Validates whether the account is owned by the declared individual.
- Account recency warnings
- Bank provider the account is with

RAG Scoring & Fraud Signals

- Ownership based fraud indicators can automatically upgrade or downgrade RAG scores depending on scenario.

Integrated ID/Bank Validation UI & Workflow

- Full ID/Bank Validation tab
- Provides validation breakdowns, match explanations, and audit logs.

Auditability & Traceability

- All inputs and outputs are logged via structured files ("ID Validations" versions).
- Supports housing, revenues, benefits, and fraud compliance teams.

5. Benefits

Fraud Prevention at Point-of-Contact

- Detects false identities, misreported bank accounts, and impersonation.
- Flags mismatches between declared occupants and actual residency patterns.



Operational Accuracy

- Ensures only legitimate applicants progress through financial support or payment-oriented workflows.
- Prevents misapplied payments by confirming bank ownership before funds are released.

Efficiency & Automation

- Automated score carding reduces manual review time.
- RAG scoring produces immediate triage outcomes.
- Clear pass/fail signals simplify officer decision making.

Improved Customer Outcomes

- Genuine applicants pass validation quickly without friction.
- Reduced need for document uploads when digital identity evidence is sufficient.

6. Maximising Impact – Synergistic Services

Ascendants services often have services which embed, compliment and significantly enhance operational efficiency. By combining services you may already have, or may wish to consider, measurable gains are possible very quickly. The following lots are example synergistic products:

- Apply4.Online® Business – Sole Trader ID Checks
- Apply4.Online® Residents – ID and Bank Checks integrated into application journeys with instant decision to require more evidence from applicants
- EARL – ID Checks for Homelessness and Housing Register Applicants

7. Service Constraints

Real – Time Validation

- Identity (name, address, DOB) and bank ownership checks update instantly, based on credit bureau APIs.
- Apply4.Online® Residents uses the same real time validation schedule for ID, bank, fraud risk scoring, and benefits crossmatching.

Scheduled or Aggregated Refresh

- Data is not refreshed



External Data & API Providers

- Credit Bureau datasets (identity corroboration, bank ownership database, DOB confirmatory checks)

Input Data Dependencies

- ID verification accuracy depends on correct name, address formatting, and DOB consistency. Apply4.Online® captures data in a valid and structured format.
- Bank checks require valid format sort code + account number, this is also enforced by Apply4.Online®

Coverage Limitations

Some accounts may not be present in bureau datasets:

- Children/youth accounts
- Newly opened accounts
- Certain niche or non-consumer banking institutions

Browser / Device Requirements

Same browser/device constraints apply across all Ascendant cloud services:

- Requires modern HTML5compliant browsers: Chrome, Edge, Firefox, Safari.
- Optimised for desktop and tablet use; mobile supported but may limit administrative tasks.
- JavaScript and cookies must be enabled (aligned with other GCloud services).
- No software installation is required — all ID & Bank checks run entirely within the Ascendant portal.

8. Onboarding & Offboarding

Onboarding

Ascendant Solutions provides a rapid and structured onboarding process for all Lot 2 Cloud Software services. Onboarding applies consistently across all products unless otherwise stated in the relevant Service Definition.

Onboarding Timescales

Subject to any third-party dependencies (for example TransUnion, Price Hubble and HM Land Registry), all Cloud Software services will be onboarded within 48 hours of contract signing.



Training

- Each purchase includes 4 hours of remote “Train the Trainer” onboarding, enabling the Buyer to confidently administer and cascade training within their organisation.
- Additional training, both remote and on-site, is available to purchase separately through our G-Cloud services. Rates are defined in the associated pricing schedule.
- Onboarding training will be provided within 5 working days, or another timeframe agreed with the Buyer.

Administration & Access

All services are self-administered. The Buyer is granted full access controls and user management rights within their tenant, enabling them to create, modify and remove users as needed.

Data Migration

Inbound data migrations are anticipated to be required for some Software Services. Where inbound migrations cannot be handled by built in tools then a scoping exercise will need to take place including a Statement of Works and a quotation for the work being completed under separate cover. Rates for Data Migration work is covered within our G Cloud listing for “Cloud Engineering and Support Services”.

Offboarding

Ascendant Solutions provides a structured, compliant offboarding process ensuring Buyers retain access to their data and receive clear notice of contractual end-of-service activities.

Contract End & Data Extraction

- A 90-day grace period is provided at the end of the contract to allow the Buyer to extract any required information prior to automatic data deletion.
- If the Buyer requires additional support or prefers to have data delivered in a different format or method this will be quoted for and billed at the Senior Engineer Development Day Rate.¹
- During this period, account managers will normally contact the Buyer to confirm requirements and to offer the option of an extended Read-Only service (available separately on G-Cloud as “Storage and Processing”).

¹ Ascendant has strict access policies and our developers cannot read data from the production systems. The Senior rate is charged for this area of expertise due to senior management involvement.



System Notifications

All users within the Buyer's tenant will receive warnings within the system when licences are approaching expiry, including reminders of data deletion risk.

Backups & Restoration

- Air-walled backups are retained for up to 6 years. These backups exist to protect both Buyer and Supplier in the event of any Data Processing compliance investigation or regulatory need.
- Following autonomous deletion, if a Buyer later requests reinstatement of their service, Ascendant Solutions will provide a time-based restoration quote calculated in accordance with our G-Cloud rate card for Senior Engineer Day Rates.
- Full-service restoration is not guaranteed and will be confirmed at the point of quote. Restoration is subject to archived data availability and authorisation by the Buyer. In scenarios where Ascendant Solutions was instructed to permanently delete tenant level cryptographic keys, restoration will not be possible.

9. Service Levels & Support

Support Hours

Support is available during normal working days, Monday to Friday, 08:00–17:00 (UK time), excluding UK Bank Holidays.

How to Log a Support Request

Buyers may raise support tickets via any of the following channels:

- Online Service Desk: <https://ascendantsol.atlassian.net/servicedesk/customer/portals>
- Telephone: 01302 543 157
- Microsoft Teams: Microsoft Organisation Tenants can call any Ascendant team member directly.

Standard Priority (Normal SLA)

Applicable to non-critical issues where service remains operational.

- Response Time: Within 2 working hour
- Resolution Target: Within 48 working hours



Critical Priority SLA

A critical issue is one that poses risk to the Buyer, Seller, or end customers, including but not limited to system outages, data related failures, or security incidents. These issues should be logged and escalated to all contacts within the Call Off contract.

- Response Time: Within 30 working minutes
- Resolution Target: Within 4 working hours

Out-of-Hours (OOH) Support

OOH support is provided for critical issues.

Escalation and OOH contact details are included within the Buyer's Call Off Contract.

Software Availability SLA

Ascendant Solutions' Cloud Software services are designed to operate "Always Online", using Microsoft Azure's high-availability architecture and design patterns which limit downtime to near zero seconds per day.

Updates as Standard

Upgrades, enhancements, security improvements or performance optimisations to our Cloud Software services are provided as standard and without additional charge. Updates are informed by a combination of customer feedback, usage analytics, and proactive application monitoring, ensuring that improvements are meaningful, stable and aligned to real world operational need. Deployments are designed to be seamless, with minimal or no service disruption, and form part of our standard commitment to maintaining secure, resilient and high performance services.

Agile Delivery & Continuous Deployment

Ascendant Solutions operates an agile, no-release-cycle development model, meaning there is no wait for new features or improvements. Instead, we use a fully automated CI/CD (Continuous Integration / Continuous Deployment) pipeline that safely deploys improvements to our live services every morning at 6am. This approach ensures that fixes, enhancements and refinements reach customers as soon as they are ready, without disruption, downtime, or the risks associated with large, infrequent updates. Our deployment process is automated, heavily tested, and designed for stability, allowing us to deliver rapid improvements based on real-time application monitoring and ongoing customer feedback. For non-technical Buyers, the practical benefit is simple: you always have the best, most secure and most up-to-date version of the service, without needing to schedule upgrades, incur extra costs, or experience outages. This continuous



improvement approach provides predictability, increased quality, faster delivery of new features, and ensures our cloud services remain aligned to evolving operational requirements.

Third-Party Dependencies Statement – Sub processors

TransUnion acts as the credit reference agency and sub processor. As part of this process, the following information is sent to and returned from TransUnion under strict data processing and security controls.

- Name
- Address
- Date of Birth
- Bank Account and Sort Code (Depending on configuration by the Buyer)

Target Availability of our Software Services

Subject to third party dependencies listed below where applicable, our target SLAs are:

- 99.9% uptime during business hours
- 99% uptime outside business hours
- Web page load times: sub second where no third-party dependency exists
- N.B. There is typically some latency of this service during high-traffic national sporting events as the service usage by the Gaming industry significantly strains the service. E.g. if England reached the World Cup or Euros final, or during the Grand National.

Ascendant's services have an embedded "Status Page" notifying user of any unexpected outages or planned maintenance. Incident and Maintenance history is available on our Status Page and Buyers are encouraged to sign up to alerts at <https://status.ascendantsol.co.uk>

10. Technical Architecture

Our Cloud Services leverage the following high-availability Azure services (each benefiting from Microsoft's own SLAs):

- Azure SQL (UK South, UK West High Availability Replica)
- Azure Firewall
- Azure Application Gateway
- Azure App Service
- Azure Storage Accounts (UK South, UK West)
- Azure App Secrets Management
- Azure Key Vault
- Azure DevOps
- Azure Pipelines
- Microsoft Entra ID for Corporate Tenant SSO (may require IT Teams to allow list)



- Amazon AWS SES “Simple Email Service” for system notifications.

These components provide built-in redundancy, automated failover where practical, and resilience appropriate for public sector workloads.

11. Information Security & Compliance

Your contracts reference:

- ISO 27001:2022 Compliant Business Management System.
- Cyber Essentials Plus
- Quantum Cryptography Readiness Plan
- Microsoft Partner
- Bi-Annual Penetration Testing
- Feature Branch Penetration Testing As Needed (e.g. Login software changes)

12. Data Protection

Ascendant Solutions Limited is committed to ensuring that all personal data processed through our cloud services is handled lawfully, securely, and transparently in accordance with the UK GDPR, Data Protection Act 2018, and all relevant public sector data protection requirements. We act as either Data Processor of your data and any data procured on your behalf via connected third party services. We act as Data Controller mainly in relation to handling your employee information as they use the services and interact with our organisation and our employees.

Roles & Responsibilities

- The Buyer is typically the Data Controller, retaining full responsibility for determining the purpose and lawful basis for processing data.
- Ascendant Solutions, when acting as the Data Processor, processes personal data strictly under the Buyer’s documented instructions, as outlined in the Call Off Contract and Data Processing Agreement.

Categories of Data Processed by Ascendant as a Data Controller

All Ascendant Services will process personal data of system users as a Data Controller. Those categories of Personal Data are:

- Name
- Email Address
- Phone Number
- Physical Address (Where using location-based services or mapping / routing)
- IP Address



- Date of Birth (Optional)
- Employment Information (Employer and Job Title)

Publicly Accessible Services

For Ascendant Services that have a publicly accessible website for use by the Buyer's customers. For example, Apply4.Online® allows residents to register to access the service without any connect to a given council. Users may register and never indicate which council they intend to fill in forms for. For this this reason, "User" or "Login" level information is controlled by Ascendant Solutions. When users of the system apply for a scheme hosted by a Buyer, the user personal data is shared with the Buyer via consent and is copied onto the Buyer Tenant Database. The Buyer is the Data Controller of that copy of the information. the user can choose to Update or Delete their user account data at any time. Updates to the Ascendant controlled data will not affect any copies of the data contained within the Buyer's control i.e. data that is contained within part-complete or submitted forms.

Categories of Data Processed by the Service as Data Processor

- Name
- Address
- Date of Birth
- Bank Account Number and Sort Code (optional)

Lawful Processing & Minimisation

Data is processed solely for purposes connected to service delivery, performance, monitoring, analytics and fraud-prevention (where applicable). We operate strict data-minimisation principles, holding only what is required to deliver the contracted service.

Security Measures

Ascendant Solutions operates within an ISO 27001 certified Business Management System, applying robust organisational and technical controls including:

- Encryption in transit and at rest
- Secure access controls and user permissions
- Air-walled backups
- Monitoring, logging and incident detection
- Controlled development and deployment pipelines
- Multi-factor authentication and Conditional access policies



- Least-privilege access and segregation of duties

Data Storage & Location

All data is stored exclusively within UK based Microsoft Azure environments. Azure services underpinning our systems benefit from high-availability, resilience and strong platform level security.

Access Control & Administration

Access to customer data is restricted to authorised personnel only, and logged for audit. Buyers are provided with full administrative control over user access within their own tenant.

Data Sharing & Sub-processors

Where services rely on third parties (e.g., TransUnion, Price Hubble, HM Land Registry), these sub-processors are listed in the Call-Off Contract or Data Processing Agreement. Ascendant ensures all sub-processors meet equivalent security and data-protection obligations.

Data Retention & Deletion

At the end of a contract, Buyers are provided with a 90-day grace period to extract any required information before automated deletion occurs.

Air walled backups are retained for up to 6 years for legal, regulatory and compliance protection. A service restoration process is possible, subject to Senior Engineer Day Rates as published on our G-Cloud service.

Data Protection Impact Assessments (DPIAs)

DPIA support is available as part of onboarding. We provide detailed information on data flows, processing activities, risks, and mitigations to enable the Buyer to satisfy their internal governance requirements.

Data Subject Rights

Ascendant supports Buyers in responding to DSARs, objections, erasure requests, rectification, and other statutory rights, ensuring timely, auditable cooperation as required. As a Data Processor we will inform you of any DSAR requests and handle them according to your instructions. Some services apply GDPR Exemptions under Schedule 2 DPA 2018 and will be identified during Onboarding and supporting you through DPIA's.



Incident Management

Ascendant maintains a documented incident response process, including:

- Immediate containment
- Assessment of scope and risk
- Notification to the Controller without undue delay
- Full forensic audit of system activity
- Support with ICO notifications if required

13. Pricing

Please refer to the associated G-Cloud pricing document for the product.

14. Service Roadmap

For information about new features and to stay up to date with the latest news, join our marketing list using the website link: <https://www.ascendantsol.co.uk/about-us/contact-us/>

15. Terms & Conditions

For T&Cs relating to use of our systems please see <https://www2.ascendantsol.co.uk/Public/TermsAndConditions>

16. Existing Users

Barking and Dagenham
Barnet
Bury
Cheshire East
Cheshire West and Chester
Dudley
Enfield
Erewash Borough Council
Hastings Borough Council
King's Lynn and West Norfolk
Milton Keynes
Oldham
Reading Borough Council
Rother



Royal Borough of Windsor and Maidenhead

Walsall

Waltham Forest

Wealden

Wolverhampton

17. Ordering, Billing & Invoicing

- Following receipt of an order, a Call Off process should be initiated in accordance with the CCS Framework.
- A Purchase Order should be generated by the Buyer at the point of contract signing for the price outlined in the Call Off.
- An invoice will be raised by the Seller upon receipt of a signed and countersigned Call Off Contract. If a purchase order number is required it should be supplied and noted within the Call Off Contract.
- Absence of a purchase order, or purchase order number, does not invalidate any orders and will not prevent invoices being raised after a reasonable grace period, normally 30 days.
- Late payment of invoices may be subject to the Late Payment of Commercial Debts Act and incur additional charges in accordance with the act.